Sullivan County

County Legislature

Meeting Agenda - Final - Revised

100 North Street
Monticello, NY 12701

Chair Nadia Rajsz
Vice Chair Luis Alvarez
Legislator Matt McPhillips
Legislator Brian McPhillips
Legislator Nicholas Salomone Jr.
Legislator Catherine Scott
Legislator Joseph Perrello
Legislator Amanda Ward
Legislator Terry Blosser-Bernardo

Thursday, May 21, 2026 **10:30 AM** **Government Center**

Call to Order and Pledge of Allegiance

Roll Call of Legislators

Presentations

Communications

Public Comment

Resolutions

1. RESOLUTION INTRODUCED BY THE PUBLIC SAFETY AND LAW ENFORCEMENT COMMITTEE TO AUTHORIZE THE COUNTY MANAGER TO ENTER INTO AN AGREEMENT TO EXPAND SERVICES PROVIDED BY TYLER TECHNOLOGIES FOR USE OF THEIR WEB CAD MONITOR INTERFACE **ID-8268**

2. TO MODIFY THE CURRENT CONTRACT BETWEEN SECURUS TECHNOLOGIES INC AND THE SULLIVAN COUNTY JAIL **ID-8311**

3. RESOLUTION INTRODUCED BY THE PLANNING AND COMMUNITY RESOURCES COMMITTEE TO AUTHORIZE THE COUNTY MANAGER TO SIGN THE 2026-2027 ANNUAL PLAN UPDATE TO THE 2024-2028 FOUR YEAR PLAN FOR THE SULLIVAN COUNTY OFFICE FOR THE AGING **ID-8326**

   Sponsors: Office for the Aging and Deoul

   Attachments: 26-27_review and approval STANDARD DATES

4. RESOLUTION INTRODUCED BY THE PUBLIC SAFETY COMMITTEE AUTHORIZING THE PREPARATION OF A GRANT APPLICATION FOR THE COMBINED SFY2025 & SFY2026 PUBLIC SAFETY ANSWERING POINT (PSAP) OPERATIONS GRANT PROGRAM WHICH IS ADMINISTERED BY THE NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES (NYS DHSES) **ID-8332**

5. To Authorize the County Manager to enter into contracts for Home Health Aides and Personal Care Aides **ID-8334**

6. Apportion the 2026 1st Quarter Mortgage Tax **ID-8339**

Attachments: AU-202 1ST QUARTER MORTGAGE TAX

7. To authorize a Contract Agreement between the County of Sullivan and Bold Gold Media Group to provide services for the Summer Youth Employment Program (SYEP) **ID-8346**

8. RESOLUTION INTRODUCED TO THE PUBLIC SAFETY AND LAW ENFORCEMENT COMMITTEE TO AUTHORIZE A SERVICE AGREEMENT WITH MOTOROLA FOR PREVENTATIVE MAINTENANCE, MAINTENANCE, SOFTWARE/HARDWARE UPGRADES AND TECHNICAL SUPPORT FOR PUBLIC SAFETY RADIO SYSTEM **ID-8348**

9. To enter into an agreement with Eastern University to permit qualified students to participate in a social work practicum experience at the Department of Community Services. **ID-8353**

10. Authorize a stipend for a District Attorney's Office Employee **ID-8361**

11. ADOPT THE "SULLIVAN COUNTY INFORMATION TECHNOLOGY AND CYBERSECURITY GOVERNANCE POLICY AND STANDARDS (SCITS-0001.000)" **ID-8362**

Attachments: Sullivan County Information Technology and Cybersecurity Governance Policy and Standards (SCITS-0001.000).pdf

12. To abandon a portion of former County Road No. 179 and convey same to the abutting landowner. **ID-8364**

Attachments: 20260514-CR179-Aband_Reso_Exhibit-Survey

13. TO AUTHORIZE A PAYMENT TO THOMSON REUTERS **ID-8365**

14. TO AUTHORIZE A 3-YEAR AGREEMENT FOR CONTINUED ACCESS TO LEXISNEXIS ADVANCE ONLINE LEGAL RESEARCH PRODUCTS **ID-8366**

15. TO AUTHORIZE A NEW THREE-YEAR AGREEMENT WITH THOMSON REUTERS FOR THEIR "CLEAR" RESEARCH PRODUCT FOR THE BENEFIT OF THE DISTRICT ATTORNEY'S OFFICE **ID-8367**

16. To authorize the County Manager to execute a contract with Payne's Cranes, Inc. for crane services needed for various Public Works Projects on an as needed basis. **ID-8369**

17. Resolution to authorize the County Manager to execute a modification agreement for engineering design services with McFarland Johnson for the 2026 Bridge Maintenance Project (PIN 9755.12) **ID-8370**

18. Resolution to authorize award and execution of agreement for Cleaning of Leachate Storage Tanks at the Sullivan County Landfill to TAM Enterprises Inc., the lowest responsible bidder for the project. **ID-8371**

19. Sullivan County Sheriff Admin & Jail facility requires fire alarm upgrade due to current system becoming obsolete, and parts being difficult or impossible to procure. **ID-8373**

20. Resolution to authorize amendments to Section 620.1 of the Sullivan County Solid Waste Management Rules. **ID-8375**

Attachments: Solid Waste Prices for consideration
Solid Waste Prices with Reso

21. To Modify the 2026 Budget **ID-8376**

Attachments: April 30 2026 Resolution Needed

22. Ratify a MOA with Teamsters Probation Unit **ID-8324**

Attachments: Probation MOA

23. Set a public hearing 6/18/26 at 8:55am to Override the NYS Property Tax Cap for 2027 **ID-8335**

Attachments: A Local Law Authorizing the Sullivan County Legislature to Override the New York State Real Property Tax Cap

24. Establish a Standard Work Day for an Elected Official **ID-8343**

25. The Legislative Discretionary Funding program is designed to assist Sullivan County and County-oriented entities with achieving such goals as public safety, public health, youth services, community development, and economic development **ID-8347**

26. Amend Resolution No, 138-26 correcting the amount **ID-8383**

27. Authorize three (3) 2027 GTSC (Governor's Traffic Safety Committee) Grant Applications **ID-8377**

28. TO APPLY FOR AND ACCEPT THE COMBINED FY2025 & FY2026 STATEWIDE INTEROPERABLE COMMUNICATIONS (SICG) FORMULA-BASED GRANT PROGRAM **ID-8381**

29. TO AUTHORIZE AN ADDITIONAL SERVICES AGREEMENT WITH JAMES McGUINNESS & ASSOCIATES, INC. FOR eSTACs IMPLEMENTATION AND SUPPORT SERVICES FOR PUBLIC HEALTH SERVICES **ID-8382**

30. Authorize contract with Sterling Environmental Engineering, P.C. to provide technical consulting with review of the Town Line Solar and Battery Storage Project **ID-8387**

Attachments: 2026-05-13_Town Line Solar RFP - Sterling Environmental Engineering_Fee Proposal

Recognition of Legislators

Announcements from Chair

Adjournment or Close

100 North Street
Monticello, NY 12701

File #: ID-8268 **Agenda Date:** 5/21/2026 **Agenda #:** 1.

Narrative of Resolution:

RESOLUTION INTRODUCED BY THE PUBLIC SAFETY AND LAW ENFORCEMENT COMMITTEE TO AUTHORIZE THE COUNTY MANAGER TO ENTER INTO AN AGREEMENT TO EXPAND SERVICES PROVIDED BY TYLER TECHNOLOGIES FOR USE OF THEIR WEB CAD MONITOR INTERFACE

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $20,600 - Grant funded - FY24 SICG

Are funds already budgeted? Choose an item.

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: Click or tap here to enter text.

Specify Compliance with Procurement Procedures:

RESOLUTION INTRODUCED BY THE PUBLIC SAFETY AND LAW ENFORCEMENT COMMITTEE TO AUTHORIZE THE COUNTY MANAGER TO ENTER INTO AN AGREEMENT TO EXPAND SERVICES PROVIDED BY TYLER TECHNOLOGIES FOR USE OF THEIR WEB CAD MONITOR INTERFACE

WHEREAS, Sullivan County 911 has been utilizing a Computer Aided Dispatch (CAD) system provided by Tyler Technologies for many years to aid in dispatching coordination, records management and response efforts; and

WHEREAS, Sullivan County 911 wishes to enhance the software through the use of their Web CAD Monitor interface which allows our user agencies access to view their CAD incident information from a web browser, and

WHEREAS, Sullivan County 911 will be utilizing grant funding received from the NYS Department of Homeland Security and Emergency Services to cover the costs associated with the software upgrade, setup and one year of maintenance, and

WHEREAS, the total cost for the software and installation is $17,240.00 with a one year maintenance costs of $3,360.00;

NOW, THEREFORE, BE IT RESOLVED, that the County Manager is hereby authorized to enter into an agreement with Tyler Technologies for the purchase and implementation of their Web CAD Monitor interface. The agreement will include setup and services cost of $17,240.00 and a one year maintenance cost of $3,360.00.

THEREFORE, BE IT FURTHER RESOLVED, that such agreement shall be approved to form by the County Attorney's office.

File #: ID-8311 **Agenda Date:** 5/21/2026 **Agenda #:** 2.

Narrative of Resolution:
TO MODIFY THE CURRENT CONTRACT BETWEEN SECURUS TECHNOLOGIES INC AND THE SULLIVAN COUNTY JAIL

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: Click or tap here to enter text.

Are funds already budgeted? Choose an item.

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: There is no cost to the County

Specify Compliance with Procurement Procedures:

INMATE TELEPHONE SERVICES

WHEREAS, Securus Technologies, Inc. currently maintains a contract with the Sullivan County Jail to provide inmate telephone services; and

WHEREAS, in 2024, the Federal Communications Commission (FCC) adopted *Incarcerated People's Communication Services; Implementation of the Martha Wright-Reed Act: Rates for Interstate Inmate Calling Services*, WC Docket Nos. 23-62 & 12-375, FCC 24-75 (released July 22, 2024) (the "2024 FCC Order"), which, among other provisions, reduced the allowable rates for voice and video communication services and prohibited providers from issuing cash or in-kind commissions derived from FCC-regulated revenues; and

WHEREAS, on June 30, 2025, the FCC issued an order (the "Waiver Order") extending the compliance deadlines for certain provisions of the 2024 FCC Order to April 1, 2027, including the implementation of new rate caps for voice and video services, the prohibition on commissions, and the requirement that video services be offered on a per-minute basis; and

WHEREAS, on December 5, 2025, the FCC published an additional order in the Federal Register (the "Interim Order"), which, among other things, modified the rate caps established in the 2024 FCC Order to account for the costs of investigative tools and safety and security services, as adjusted for inflation, and authorized a per-minute additive to recover costs incurred by correctional facilities in providing access to incarcerated people's communication services; and

WHEREAS, a modification to the existing contract is necessary to ensure compliance with applicable FCC regulations; and

WHEREAS, Securus Technologies, LLC has proposed enhancements, including upgraded technology and investigative features, to improve the safety and security of inmate communications; and

WHEREAS, Securus Technologies, LLC has agreed to provide these enhancements at no additional cost to

Sullivan County in exchange for an extension of the current contract term from 2030 to 2033;

NOW, THEREFORE, BE IT RESOLVED, that the County Manager is hereby authorized to execute a modification agreement with Securus Technologies, LLC to extend the existing contract for inmate telephone services through the year 2033 and this agreement shall be approved as to form by the County Attorney's Office and

BE IT FURTHER RESOLVED, that such modification agreement shall incorporate all necessary provisions to ensure compliance with applicable FCC regulations and to implement the proposed technological and security enhancements.

File #: ID-8326 **Agenda Date:** 5/21/2026 **Agenda #:** 3.

Narrative of Resolution:
TO AUTHORIZE THE COUNTY MANAGER TO SIGN THE 2026-2027 ANNUAL PLAN UPDATE TO THE 2024-2028 FOUR YEAR PLAN FOR THE SULLIVAN COUNTY OFFICE FOR THE AGING

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: 0

Are funds already budgeted? Choose an item.

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: Click or tap here to enter text.

Specify Compliance with Procurement Procedures:

RESOLUTION INTRODUCED BY THE PLANNING AND COMMUNITY RESOURCES COMMITTEE TO AUTHORIZE THE COUNTY MANAGER TO SIGN THE 2026-2027 ANNUAL PLAN UPDATE TO THE 2024-2028 FOUR YEAR PLAN FOR THE SULLIVAN COUNTY OFFICE FOR THE AGING

WHEREAS, the Sullivan County Office for the Aging administers programs funded under the Older Americans Act (Title III), Wellness in Nutrition, the New York State Community Services for the Elderly Program, the Expanded In-Home Services for the Elderly Program, the Congregate Services Initiative, the State Transportation Program, the Caregiver Resource Center, the Health Insurance Information Counseling and Assistance Program, and Unmet Needs Funding, which authorize the expenditure of Federal and State funds to provide services for older residents of Sullivan County; and

WHEREAS, State and Federal regulations require the County to prepare and submit an Annual Plan outlining the services to be provided under the above-mentioned programs; and WHEREAS, the New York State Office for the Aging requires submission of a Four-Year Plan for the period 2024-2028, with annual updates including funding applications, plan reviews, and related documentation; and

WHEREAS, the Sullivan County Office for the Aging has prepared the 2026-2027 Annual Plan Update to the 2024-2028 Four-Year Plan; and

WHEREAS, the regulations require the County Manager to sign the Annual Plan Update in order for the County to receive Federal and State funding allocations;

NOW, THEREFORE, BE IT RESOLVED, that the County Manager be and hereby is authorized to sign any and all applications, agreements, and documents necessary to implement the Sullivan County Office for the Aging 2026-2027 Annual Plan Update to the 2024-2028 Four-Year Plan; and

BE IT FURTHER RESOLVED, that such applications and agreements shall be in a form approved by the Sullivan County Department of Law; and

BE IT FURTHER RESOLVED, that all commitments and agreements are contingent upon receipt of the necessary

Federal and State allocations; and

BE IT FURTHER RESOLVED, that should Federal and/or State funding, including Older Americans Act (Title III) funding, be terminated, the County shall not be obligated to continue any actions or services initiated through the use of such funding.

ANNUAL UPDATE REVIEW AND APPROVAL

Must be signed by the AAA Director (and the Chief Officer of the Governing Body of the Sponsoring Organization if the other than County, New York City, or Native American Organization).

I hereby submit for approval the Four Year Plan and the annual Applications for Funding (hereafter referred to as the Plan) for Older Americans Act (OAA) programs, New York State Community Services for the Elderly (CSE) Program and Expanded In-Home Services for the Elderly Program (EISEP), and the applications for funding indicated below:

Program	Program Period	Program Applied For
Title III-B	January 1, 2026 to December 31, 2026	□Yes □No
Title III-C	January 1, 2026 to December 31, 2026	□Yes □No
Title III-D	January 1, 2026 to December 31, 2026	□Yes □No
Title III-E	January 1, 2026 to December 31, 2026	□Yes □No
EISEP	April 1, 2026 to March 31, 2027	□Yes □No
CSE	April 1, 2026 to March 31, 2027	□Yes □No
CSI	April 1, 2026 to March 31, 2027	□Yes □No
WIN	April 1, 2026 to March 31, 2027	□Yes □No
Unmet Need	April 1, 2026 to March 31, 2027	□Yes □No
Transportation	April 1, 2026 to March 31, 2027	□Yes □No
CRC	April 1, 2026 to March 31, 2027	□Yes □No
HIICAP	April 1, 2026 to March 31, 2027	□Yes □No

I agree to comply with all applicable federal, state and local laws and regulations, program standards, and standard assurances which affect any funds, (including matching funds and program income) used for the programs described in this Plan. I have read and agree to comply with all of the Standard Assurances (Attachment A) in the Plan. In addition, I certify that no amendments have been made nor will be made to the Standard Assurances in the Plan. Furthermore, I agree to comply with all attachments submitted as part of this Plan and indicated on the Attachment Checklist.

I also certify that the information contained in the Priority Services Schedule (Attachment B) is true and correct.

I also certify that this organization is not currently suspended or debarred as defined in 2 CFR part 376.

_____ _____ _____
Signature of AAA Director Print/Type Name Date

_____ _____
Signature of the Chief Executive Officer of the Governing Body of the Sponsoring Organization (if other than County, New York City, or Native American Organization) Date

_____ _____
Print/Type Name Print/Type Title

LOCAL GOVERNMENT EXECUTIVE REVIEW AND APPROVAL

Must be signed ONLY if the AAA intends to apply for CSE program or EISEP state aid pursuant to the New York State Elder Law.

I, _____ being the Chief Executive Officer of the Governing Board of
Print/Type Name
this _____(County, New York City, or Native American Organization), do hereby certify that:

1. The _____, an AAA established pursuant to the OAA of 1965, as amended, has been duly designated by me pursuant to New York State Elder Law §214.

[ ] CSE
[ ] EISEP

2. This Plan for the OAA and New York State CSE and/or EISEP pursuant to New York State Elder Law, is hereby approved for submission to the New York State Office for the Aging.

_____ _____ _____
Signature (*Use ink."per" signature not acceptable*) Print/Type Title Date

File #: ID-8332 **Agenda Date:** 5/21/2026 **Agenda #:** 4.

Narrative of Resolution:

RESOLUTION INTRODUCED BY THE PUBLIC SAFETY COMMITTEE AUTHORIZING THE PREPARATION OF A GRANT APPLICATION FOR THE COMBINED SFY2025 & SFY2026 PUBLIC SAFETY ANSWERING POINT (PSAP) OPERATIONS GRANT PROGRAM WHICH IS ADMINISTERED BY THE NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES (NYS DHSES)

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $306,892.00 (Grant funds)

Are funds already budgeted? No

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: Public Safety Answering Point (PSAP) Operations Grant

Specify Compliance with Procurement Procedures:

RESOLUTION INTRODUCED BY THE PUBLIC SAFETY COMMITTEE AUTHORIZING THE PREPARATION OF A GRANT APPLICATION FOR THE COMBINED SFY2025 & SFY2026 PUBLIC SAFETY ANSWERING POINT (PSAP) OPERATIONS GRANT PROGRAM WHICH IS ADMINISTERED BY THE NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES (NYS DHSES)

WHEREAS, the New York State Division of Homeland Security and Emergency Services (NYS DHSES) provides funds to support efforts of public safety answering point operations; and

WHEREAS, the NYS DHSES - Office of Interoperable and Emergency Communications (OIEC), is administering the combined SFY2025 & SFY2026 Public Safety Answering Point (PSAP) operations grant program; and

WHEREAS, The FY25-26 Public Safety Answering Point grant is a reimbursement based program; and

WHEREAS, the Sullivan County Division of Public Safety - E911 Communications Department has been deemed eligible for $306,892.00 in funding to support the improvement of public safety communications and PSAP operations for the performance period of 1/1/2026 - 12/31/2028; and

WHEREAS, the Sullivan County Division of Public Safety - E911 Communications Department must submit an application in order to receive said funds and wishes to file an application with the PSAP program; and

WHEREAS, Sullivan County is not required to provide a local cash or in-kind match in support of the PSAP program.

NOW THEREFORE BE IT RESOLVED, that the Sullivan County Division of Public Safety - E911 Communications Department is hereby authorized to prepare an application for said funding under the NYS DHSES OIEC PSAP program.

BE IT FURTHER RESOLVED, that the Sullivan County Legislature hereby authorizes the County Manager to execute any and all necessary documents to submit the combined SFY 2025 & SFY 2026 NYS DHSES OIEC PSAP operations grant program application for said funding; and

BE IT FURTHER RESOLVED, that the Sullivan County Legislature hereby authorizes the County Manager to accept the award, and enter into an award agreement or contract to administer the funding secured, in such form as the County Attorney shall approve; and

BE IT FURTHER RESOLVED, that if awarded PSAP operations grant program funding, the Sullivan County Division of Public Safety - E911 Communications Department, shall administer the funds and grant program; and

BE IT FURTHER RESOLVED, that should the PSAP operations grant program funding program be terminated, the County shall not be obligated to continue any action undertaken by the use of this funding.

File #: ID-8334 **Agenda Date:** 5/21/2026 **Agenda #:** 5.

Narrative of Resolution:
To Authorize the County Manager to enter into contracts for Home Health Aides and Personal Care Aides
If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: Rate to agency is $40 with guaranteed minimum of $24 to the aide, hourly.

Are funds already budgeted? Yes

If 'Yes,' specify appropriation code(s): 7610-87-40-4024

If 'No,' specify proposed source of funds: N/A

Specify Compliance with Procurement Procedures: RFP-#R-26-13

RESOLUTION INTRODUCED BY HEALTH AND HUMAN SERVICES COMMITTEE TO AUTHORIZE AWARD & EXECUTION OF CONTRACTS WITH FOUR (4) CONTRACTORS FOR PERSONAL CARE AND HOME HEALTH CARE AIDES

WHEREAS, Request for Proposal #R-26-13 was issued and proposal's were received for Personal Care and Home Health Aides for Sullivan County; and

WHEREAS, the following Contractors will provide said services for Home Health Aide and Personal Care Aide at an hourly rate of $40.00, with a guaranteed minimum of $24.00/hour to the aide for the contract period of July 1,2026 through June 30, 2027, with an option to extend on a yearly basis, for four (4) additional years, under the same terms and conditions; and

A & T Healthcare, LLC
339 North Main Street
New City, NY 10956
Spring Valley, NY 10956

Any-Time Healthcare, Inc.
9 ½ Dolson Avenue
Middletown, NY 10940

Community Health Aide Services, Inc.
49 N Airmont Road
Montebello, NY 10901

Willcare Inc. d/b/a Willcare

726 East Main Street

Suite 303

Middletown, NY 10940

WHEREAS, the Sullivan County Department of Public Health recommends said contractors.

NOW, THEREFORE, BE IT RESOLVED, that the County Manager be and hereby is authorized to execute the contracts with the above contractors, at the above referenced rates, in accordance with RFP-#R-26-13; for the contract period of July 1,2026 through June 30, 2027, with an option to extend on a yearly basis, for four (4) additional years, under the same terms and conditions; said contracts to be in such form as the County Attorney shall approve.

File #: ID-8339 **Agenda Date:** 5/21/2026 **Agenda #:** 6.

Narrative of Resolution:
Apportion the 2026 1st Quarter Mortgage Tax

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: N/A

Are funds already budgeted? Choose an item.

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: Click or tap here to enter text.

Specify Compliance with Procurement Procedures:

RESOLUTION INTRODUCED BY MANAGEMENT AND BUDGET COMMITTEE TO APPORTION MORTGAGE TAX

WHEREAS, Section 261 of the Tax Law of the State of New York requires apportionment of the mortgage tax, and

WHEREAS, the County Clerk and the County Treasurer have submitted the quarterly report to the Clerk of the Legislature, and

WHEREAS, The County Legislature has apportioned, among the various towns and incorporated villages of the County of Sullivan, the equitable share of the mortgage tax;

NOW, THEREFORE, BE IT RESOLVED, that the County Treasurer draw checks for each of the towns and villages the quarterly mortgage tax so apportioned, for the 1st Quarter 2026, as follows:

TOWNS

Bethel	$54,764.26
Callicoon	$19,716.25
Cochecton	$13,464.59
Delaware	$18,803.50
Fallsburg	$226,978.77

Forestburgh	$10,864.45
Fremont	$11,986.49
Highland	$31,972.93
Liberty	$73,696.77
Lumberland	$40,258.17
Mamakating	$71,750.98
Neversink	$9,662.58
Rockland	$33,136.39
Thompson	$209,962.08
Tusten	$15,440.89

VILLAGES

Bloomingburg	$2,309.44
Jeffersonville	$1,165.78
Liberty	$12,729.74
Monticello	$22,146.36
Woodridge	$7,507.88
Wurtsboro	$2,929.32
Ateres - F	$98.08
Ateres - T	$1,533.40
TOTAL	**$892,879.10**

New York State Mortgage Tax Semi-Annual/Quarterly Report
County of Sullivan for the period: January 2026 through March 2026
Cash Statement for Taxes Collected Pursuant to Article 11

Months	BASIC TAX DISTRIBUTED					TREASURER			ALL OTHER TAXES DISTRIBUTED				
	1 Basic tax collected	2 Interest received by recording officer	3 Recording officer's expense	4 Refunds or adjustments	5 Amount paid to treasurer (Col 1+2-3-4)	6 Interest received by treasurer	7 Treasurer's expense	8 Tax districts share (Col. 5+6-7)	9 Local tax	10 Additional tax	11 Special Assistance fund	12 Special additional tax	13 County Tax
October					$ -			$ -					
November					$ -			$ -					
December					$ -			$ -					
January	$ 321,664.00	$ 366.95	$ 3,812.83	$ -	$ 318,218.12	$ 769.99	$ -	$ 318,988.11	$ 159,109.06			$ 152,128.75	
February	$ 283,077.91	$ 334.65	$ 3,821.76	$ -	$ 279,590.80	$ 934.44		$ 280,525.24	$ 139,795.42			$ 131,927.86	
March	$ 295,661.13	$ 272.05	$ 3,799.19		$ 292,133.99	$ 1,231.76		$ 293,365.75	$ 145,887.15			$ 142,200.92	
April				$ -	$ -		$ -	$ -					
May					$ -		$ -	$ -					
June				$ -	$ -			$ -					
July					$ -			$ -					
August					$ -			$ -					
September					$ -			$ -					
TOTALS	$ 900,403.04	$ 973.65	$ 11,433.78	$ -	$ 889,942.91	$ 2,936.19	$ -	$ 892,879.10	$ 444,791.63	$ -	$ -	$ 426,257.53	$ -

Russell Rec — Sullivan County Clerk

Kathleen Lara — Sullivan County Treasurer

AU-202

100 North Street
Monticello, NY 12701

File #: ID-8346 **Agenda Date:** 5/21/2026 **Agenda #:** 7.

Narrative of Resolution:
To authorize a Contract Agreement between the County of Sullivan and Bold Gold Media Group to provide services for the Summer Youth Employment Program (SYEP)

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $33,000.00 annually

Are funds already budgeted? Yes

If 'Yes,' specify appropriation code(s): A-6293-R4789-R314

If 'No,' specify proposed source of funds:

Specify Compliance with Procurement Procedures: RFP #24-20 & Resolution 294-24

RESOLUTION INTRODUCED BY THE ECONOMIC DEVELOPMENT COMMITTEE TO AUTHORIZE A CONTRACT AGREEMENT BETWEEN THE COUNTY OF SULLIVAN AND BOLD GOLD MEDIA GROUP

WHEREAS, the Center for Workforce Development (CWD) runs the Summer Youth Employment Program (SYEP) under the MOU with the County of Sullivan Department of Social Services (DSS) through funds provided by the New York State Office of Temporary and Disability Assistance (OTDA), and

WHEREAS, participants must be engaged in traditional paid employment activities such as career exploration, mentoring, financial literacy, or education. CWD is requesting to enter into a contract with Bold Gold Media Group, to provide the education service component for the SYEP through life skills, hard and soft skill training, and occupational skills training in multimedia as a business, to include branding concepts, broadcast marketing; digital graphics, video and audio; visualization; photography; website development; social media; radio; podcasting; industry professionalism; and more; and

WHEREAS, under RFP #R-24-20 CWD has the right to extend this agreement for an additional four (4) years, on a yearly basis, in an amount not to exceed $33,000 annually; and

NOW, THEREFORE, BE IT RESOLVED, that the County Manager is hereby authorized to enter into a contract with Bold Gold Media Group for the six-week SYEP schedule, from July 6, 2026 through August 14, 2026, in an amount not to exceed $33,000 annually, and such contract shall be in the form approved by the County Attorney. This contract is extendable for an additional (3) years, on a yearly basis, for dates and funding to be determined, and is contingent each year on CWD receiving all funding.

File #: ID-8348 **Agenda Date:** 5/21/2026 **Agenda #:** 8.

Narrative of Resolution:
RESOLUTION INTRODUCED TO THE PUBLIC SAFETY AND LAW ENFORCEMENT COMMITTEE TO AUTHORIZE A SERVICE AGREEMENT WITH MOTOROLA FOR PREVENTATIVE MAINTENANCE, MAINTENANCE, SOFTWARE/HARDWARE UPGRADES AND TECHNICAL SUPPORT FOR PUBLIC SAFETY RADIO SYSTEM

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution:
2026 - 2027: $625,574.37
2027 - 2028: $657,683.00
2028 - 2029 $696,445.54
2029 - 2030 $731,828.54
2030 - 2031 $756,273.51

Are funds already budgeted? Yes

If 'Yes,' specify appropriation code(s): Source Grant for April 1 - December 2026

If 'No,' specify proposed source of funds: January 1 - March 31, 2027 pending grant and/or budget appropriation

Specify Compliance with Procurement Procedures:

RESOLUTION INTRODUCED TO THE PUBLIC SAFETY AND LAW ENFORCEMENT COMMITTEE TO AUTHORIZE A SERVICE AGREEMENT WITH MOTOROLA FOR PREVENTATIVE MAINTENANCE, MAINTENANCE, SOFTWARE/HARDWARE UPGRADES AND TECHNICAL SUPPORT FOR PUBLIC SAFETY RADIO SYSTEM

WHEREAS, Sullivan County's 911 radio system, which is the primary component for handling and dispatching emergency service calls, is in need of preventative maintenance, maintenance, software & hardware upgrades, and technical support to allow for continued communications and interoperability, and

WHEREAS, This is a continuation for services authorized by Resolution #426-19 which covered years 2019-2026, and

WHEREAS, It is essential that the County maintain its radio system and infrastructure in a constant state of readiness and high availability, and

WHEREAS, Motorola is the sole source vendor to be able to provide these services as the system manufacturer,

NOW THEREFORE BE IT RESOLVED, that the County Manager, upon review and approval by the County

Attorney's office and subject to annual appropriation of funding, be and hereby is authorized to sign the maintenance, support and software & hardware agreement with Motorola subject to the following fee schedule for the years of 2026-2031:

2026 - 2027: $625,574.37
2027 - 2028: $657,683.00
2028 - 2029 $696,445.54
2029 - 2030 $731,828.54
2030 - 2031 $756,273.51

100 North Street
Monticello, NY 12701

Sullivan County

Legislative Memorandum

File #: ID-8353 **Agenda Date:** 5/21/2026 **Agenda #:** 9.

Narrative of Resolution:
To enter into an agreement with Eastern University to permit qualified students to participate in a social work practicum experience at the Department of Community Services.
If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $0

Are funds already budgeted? No

If 'Yes,' specify appropriation code(s): N/A

If 'No,' specify proposed source of funds: N/A

Specify Compliance with Procurement Procedures:

To permit qualified students to participate in a social work practicum experience at the Department of Community Services.

RESOLUTION INTRODUCED BY HEALTH AND HUMAN SERVICES TO ENTER INTO AGREEMENT WITH EASTERN UNIVERSITY TO PERMIT QUALIFIED STUDENTS TO PARTICIAPTE IN A SOCIAL WORK PRACTICUM EXPERIENCE AT THE DEPARTMENT OF COMMUNITY SERVICES

WHEREAS, Eastern University ("University") maintains a program which awards a degree in Social Work and wishes to assign students to the Department of Community Services ("DCS") for practical experience; and

WHEREAS, DCS wishes to enter into an agreement with the University to permit qualified students to participate in said educational program.

NOW, THEREFORE, BE IT RESOLVED , that the County Manager is hereby authorized to enter into an agreement with Eastern University for the period from May 1, 2026 through April 30, 2027. Thereafter, the agreement shall automatically renew from year to year unless terminated through written notice at the end of any contract year, as set forth in the terms of the agreement; and

BE IT FURTHER RESOLVED, that the form of said agreement shall be approved by the Sullivan County Attorney's Office.

100 North Street
Monticello, NY 12701

File #: ID-8361 **Agenda Date:** 5/21/2026 **Agenda #:** 10.

Narrative of Resolution:
Authorize a stipend for a District Attorney's Office Employee

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $10,000

Are funds already budgeted? Yes

If 'Yes,' specify appropriation code(s): R3089-R167

If 'No,' specify proposed source of funds:

Specify Compliance with Procurement Procedures

RESOLUTION INTRODUCED BY PUBLIC SAFETY AND LAW ENFORCEMENT COMMITTEE TO AUTHORIZE A STIPEND FOR A DISTRICT ATTORNEY'S OFFICE EMPLOYEE TO SUPPORT COUNTYWIDE PROJECT IMPLEMENTATION AND DISCOVERY COMPLIANCE

WHEREAS, the New York State Division of Criminal Justice Services (DCJS) provides funding to counties to offset costs associated with the implementation and ongoing compliance with discovery and pretrial reforms; and

WHEREAS, Sullivan County has received NYS DCJS Discovery Reform funding, including available fund balance under account R3089-R167, to support prosecutorial and law enforcement functions necessary to meet these mandates; and

WHEREAS, the implementation of countywide systems and initiatives, including but not limited to NicheRMS, requires dedicated administrative coordination, project support, and interagency collaboration beyond the scope of existing job duties; and

WHEREAS, discovery reform requires compliance with Brady and Giglio obligations that require intensive and coordinated efforts between the District Attorney's Office and five separate law enforcement agencies to organize, file, and review all civil litigation as well as all disciplinary findings which are beyond the scope of existing job duties; and

WHEREAS, such efforts directly support the District Attorney's Office in meeting its obligations under New York State Discovery laws, including the identification, management, and disclosure of Brady/Giglio materials, as well as ensuring litigation readiness and compliance; and

WHEREAS, it is necessary to designate and compensate a qualified employee within the District Attorney's Office to assume these additional responsibilities in support of countywide project implementation and discovery compliance;

NOW, THEREFORE, BE IT RESOLVED, that the Public Safety Committee recommends that the Sullivan County Legislature authorize a $10,000 stipend to be paid to a District Attorney's Office employee, Position No. 2968, for the purpose of supporting countywide project implementation, including NicheRMS, and advancing discovery and Brady compliance efforts; and

BE IT FURTHER RESOLVED, that said stipend shall be funded from NYS DCJS Discovery Reform funds, specifically fund balance account R3089-R167, resulting in no cost to the County; and

BE IT FURTHER RESOLVED, that the County Manager and/or Chair of the Sullivan County Legislature, as required by the funding source, are hereby authorized to execute any and all documents necessary to effectuate this resolution; and

BE IT FURTHER RESOLVED, that in the event NYS DCJS Discovery Reform funding is terminated, the County shall not be obligated to continue the stipend or any actions supported by said funding.

File #: ID-8362 **Agenda Date:** 5/21/2026 **Agenda #:** 11.

Narrative of Resolution:
This resolution adopts a fully modernized and consolidated information technology and cybersecurity governance framework for Sullivan County. The policy replaces fragmented and outdated guidance with a single, unified standard that establishes clear authority, consistent requirements, and County-wide accountability. The framework aligns with applicable State and Federal regulations and incorporates recognized cybersecurity best practices to address the increasing risk of ransomware, data breaches, and system disruption. It also improves operational consistency, simplifies administration, and strengthens the County's ability to respond to incidents in a coordinated and defensible manner. By adopting this policy, the County enhances protection of sensitive information, supports continuity of operations, and ensures a clear, enforceable structure for managing technology and cybersecurity risks across all departments.

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $0

Are funds already budgeted? Choose an item.

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: Click or tap here to enter text.

Specify Compliance with Procurement Procedures:

RESOLUTION INTRODUCED BY THE MANAGEMENT & BUDGET COMMITTEE ADOPTING THE "SULLIVAN COUNTY INFORMATION TECHNOLOGY AND CYBERSECURITY GOVERNANCE POLICY AND STANDARDS (SCITS-0001.000)"

WHEREAS, Sullivan County relies on information technology systems, networks, applications, and data to conduct essential government operations and deliver public services, and such systems and data are critical public assets that must be protected from unauthorized access, misuse, disruption, and evolving cybersecurity threats; and

WHEREAS, the increasing frequency, sophistication, and impact of cybersecurity threats require a coordinated, risk-based, and enterprise-wide approach to information security; and

WHEREAS, Sullivan County's Division of Information Technology Services has undertaken a comprehensive modernization of its information technology and cybersecurity policies to strengthen governance, improve internal controls, enhance accountability, and align with applicable federal and New York State laws, regulations, and industry standards; and

WHEREAS, the resulting *Sullivan County Information Technology and Cybersecurity Governance Policy and Standards (SCITS-0001.000)* establishes a unified, county-wide framework that consolidates previously separate policies into a single, authoritative document to improve consistency, clarity of authority, and implementation across all departments; and

WHEREAS, the policy establishes centralized oversight by the Commissioner of Information Technology / Chief Information Officer (CIO) and is designed to strengthen the County's ability to protect sensitive information, maintain continuity of operations, meet legal and regulatory obligations, and respond effectively to cybersecurity incidents.

NOW THEREFORE BE IT RESOLVED, that the Sullivan County Legislature hereby adopts the Sullivan County Information Technology and Cybersecurity Governance Policy and Standards (SCITS-0001.000), effective immediately; and

BE IT FURTHER RESOLVED, that this policy shall serve as the County's authoritative standard for information technology governance, cybersecurity, operational controls, and acceptable use of County technology resources; and

BE IT FURTHER RESOLVED, that all County departments, employees, contractors, and authorized users shall comply with the provisions of this policy; and

BE IT FURTHER RESOLVED, that the Commissioner of Information Technology / Chief Information Officer is authorized to administer, implement, maintain, and enforce this policy, and to issue supporting standards and procedures as necessary; and

BE IT FURTHER RESOLVED, that this policy supersedes all prior information technology and cybersecurity policies inconsistent with its provisions.

SULLIVAN COUNTY

Information Technology And Cybersecurity Governance Policy and Standards

SCITS-0001.000

Issued: May 2026

Sullivan County Division of Information Technology Services

Sullivan County Government Center

100 North Street

Monticello, New York 12701

845-807-0110

helpdesk@sullivanny.gov

Executive Summary

Sullivan County Information Technology Services has developed and adopted a comprehensive, unified framework governing information technology, cybersecurity, operational controls, and acceptable use of County technology resources. This document represents a complete modernization and consolidation of practices and policies into a single, authoritative standard designed to document, strengthen security, improve accountability, and support consistent operations across all County departments.

This policy establishes clear lines of authority, including centralized oversight by the Commissioner of Information Technology / Chief Information Officer (CIO), while aligning responsibilities across County leadership, departments, and users. It incorporates a risk-based, Zero Trust approach to cybersecurity and aligns with applicable federal and New York State laws, regulatory requirements, and recognized industry standards, including NIST, CJIS, HIPAA, and other Federal and NYS cybersecurity guidance.

The document is intentionally structured as an integrated, all-in-one policy rather than a collection of separate documents. This approach reduces fragmentation, eliminates conflicting requirements, and ensures that all users and departments operate under a consistent and clearly defined set of expectations. By consolidating governance, technical controls, and acceptable use requirements into a single framework, the County improves administrative efficiency, simplifies training and enforcement, and enhances audit readiness.

Intentional redundancy is incorporated throughout the document to ensure that individual sections and policies can function independently when distributed, referenced, or enforced. This design supports clarity, reduces misinterpretation, and ensures that critical requirements remain visible and enforceable regardless of how the document is accessed or applied.

This framework strengthens the County's ability to:

- Protect sensitive and critical information assets from evolving cybersecurity threats;
- Ensure continuity of essential government operations;
- Meet legal, regulatory, and contractual obligations;
- Provide clear expectations for appropriate use and accountability; and
- Support rapid, coordinated, and defensible response to cybersecurity incidents.

By adopting this unified policy, Sullivan County establishes a durable governance model that enhances security, reduces operational and legal risk, and positions the County to adapt effectively to future technological, regulatory, and threat landscape changes.

This document serves as the County's authoritative standard for information technology governance and cybersecurity and is intended to support both daily operations and long-term strategic resilience.

How This Document Is Structured

This document establishes Sullivan County's unified framework for information technology governance, cybersecurity, operational controls, and acceptable use of County technology resources. It is intentionally designed as a single, comprehensive policy to promote consistency, clarity of authority, and ease of administration across all County departments.

For ease of understanding, implementation, and auditability, the document is organized into numbered sections and control domains that group related requirements by function and security objective.

Section 1 — Information Technology Governance

This section defines the County's governance model, authority structure, and overall approach to information security, risk management, accountability, and oversight.

It establishes:

- the role and authority of the Commissioner of Information Technology / Chief Information Officer (CIO);
- departmental responsibilities and accountability for information assets and internal controls;
- the County's risk-based, Zero Trust approach to cybersecurity; and
- the legal, regulatory, and operational framework governing County technology use.

This section is intended primarily for County leadership, Department Heads, and individuals with governance, operational, or oversight responsibilities.

Section 2 — Information Technology Policy, Guidelines, and Procedures

This section explains the policy framework used throughout the document and establishes how supporting standards, procedures, and control domains are organized.

It provides:

- an overview of the County's policy structure;
- the relationship between governance requirements, technical controls, and acceptable use expectations; and
- the numbering framework used to organize policies by subject matter and control objective.

This section serves as the structural bridge between the County's governance requirements and the detailed policies that follow.

Section 3 — Identity and Access Management (3000 Series)

This section establishes requirements governing user identity, account administration, credentials, authentication, and privileged access.

It includes policies addressing:

- network identification and account assignment;
- account maintenance and lifecycle management;
- password and credential requirements;
- multi-factor authentication; and
- privileged access management.

These policies are intended to ensure that access to County systems and data is authorized, attributable, and appropriately controlled.

Section 4 — Asset and Data Governance (4000 Series)

This section establishes requirements for the classification, storage, backup, retention, tracking, disposal, and protection of County information and technology assets.

It includes policies governing:

- data classification and handling;
- data storage;
- data backup and recovery;
- data retention and archiving;
- asset inventory and tracking;
- asset disposal and destruction; and
- removable media and portable storage.

These policies are intended to support confidentiality, integrity, availability, recoverability, and lifecycle accountability for County data and technology resources.

Section 5 — Network and Infrastructure Security (5000 Series)

This section establishes security requirements for County networks, connectivity, remote access, wireless access, and endpoint protection.

It includes policies governing:

- network access;
- remote access;
- wireless network security; and
- endpoint protection and malware defense.

These policies are intended to protect County infrastructure from unauthorized access, compromise, disruption, and misuse.

Section 6 — Acceptable Use and User Responsibilities (6000 Series)

This section defines the appropriate and prohibited use of County technology resources by all authorized users.

It includes policies governing:

- email;
- Internet resources;
- mobile devices;
- telephony services;
- social media;
- instant messaging;
- cloud services and storage; and
- printers and copiers.

This section applies to all employees, elected officials, contractors, consultants, vendors, and other individuals granted access to County systems or data.

Section 7 — System and Application Security (7000 Series)

This section establishes requirements for securing software, applications, specialized technology tools, and related operational use.

It includes policies governing:

- software installation and management;
- email encryption;
- application security and development; and
- the use of Artificial Intelligence (AI) in County operations.

These policies are intended to ensure that systems and applications are deployed, managed, and used in a secure, controlled, and legally compliant manner.

Section 8 — Third-Party, Vendor, and External Asset Control (8000 Series)

This section establishes requirements for external access, technology procurement, technology acquisition, domain management, and cloud-related risk review.

It includes policies governing:

- third-party access;
- technology services procurement;
- technology equipment and software acquisition;
- Domain Name System (DNS) and domain registration; and
- cloud services risk and approval.

These policies are intended to ensure that third-party relationships, external services, and externally managed technology assets are subject to centralized oversight and appropriate security review.

Section 9 — Incident Response and Security Operations (9000 Series)

This section establishes requirements for incident detection, response, breach reporting, monitoring, logging, and recovery prioritization.

It includes policies governing:

- incident response and cybersecurity event management;
- security breach notification and reporting;
- security monitoring and logging; and
- disaster recovery and system prioritization.

These policies are intended to support timely escalation, coordinated response, legal and regulatory compliance, and restoration of County operations following disruption or compromise.

Section 10 — Operational and Administrative Controls (10000 Series)

This section establishes administrative and operational requirements supporting the day-to-day management of County technology services and user accountability.

It includes policies governing:

- IT service requests and support;
- system notification and alerting;
- security awareness, training, and testing;
- phishing simulation and testing; and
- County equipment use and accountability.

These policies support consistent service delivery, user preparedness, operational discipline, and organizational accountability.

Appendices and Supporting Materials

The appendices include required acknowledgements, compliance summaries, agreements, definitions, and other supporting materials that assist with implementation, interpretation, and administration of this document.

Unified Policy Approach

This document is intentionally maintained as a single, authoritative source of information technology governance, cybersecurity, operational control, and acceptable use policy.

While some organizations maintain these elements in separate documents, Sullivan County adopts a unified structure in order to:

- ensure consistency across all requirements;
- maintain clear lines of authority and accountability;
- reduce fragmentation and conflicting interpretations; and
- support efficient administration, enforcement, and audit readiness.

All users and departments are expected to comply with the provisions applicable to their roles and responsibilities.

This document constitutes Sullivan County's authoritative and controlling policy for information technology governance, cybersecurity, and the protection of County information systems and data.

Related Standards and Governing Authorities

This policy and the associated Information Technology Governance and Employee Handbook for Information Security are aligned with, and informed by, applicable federal, New York State, and industry standards, including but not limited to the following:

- New York State Standards and Guidance
- New York State Cyber Security Policy NYS-P03-002
- New York State Information Classification Standard NYS-S14-001
- New York State Acceptable Use of Information Technology Resources Policy NYS-P10-002
- New York State Information Security Breach and Notification Act (General Business Law §899-aa; State Technology Law §208)
- New York State Office of Information Technology Services (ITS) Security Policies and Standards
- New York State Office of the State Comptroller (OSC) – Local Government Management Guide: Information Technology Governance
- New York State Archives (SARA) – Records Retention and Disposition Schedule LGS-1
- New York State Freedom of Information Law (FOIL) (Public Officers Law, Article 6)
- New York State Electronic Signatures and Records Act (ESRA) (9 NYCRR Part 540)
- New York State Civil Service Law
- Federal Laws and Regulatory Frameworks
- Federal Rules of Civil Procedure (eDiscovery and records preservation)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- 42 CFR Part 2 (Confidentiality of Substance Use Disorder Patient Records), where applicable
- Criminal Justice Information Services (CJIS) Security Policy (latest version)
- Payment Card Industry Data Security Standard (PCI DSS)
- Internal Revenue Service (IRS) Publication 15-B
- Healthcare Regulatory Requirements (Article 28 and Related Obligations)
- New York State Article 28 Diagnostic and Treatment Center Regulations (10 NYCRR)
- New York State Department of Health (NYSDOH) privacy, security, and breach reporting requirements applicable to County-operated healthcare services
- Health Insurance Portability and Accountability Act (HIPAA) and HITECH, as applied to covered entities and business associates
- 42 CFR Part 2, where applicable to substance use disorder services
- For County-operated healthcare services, including Article 28 facilities, the most stringent applicable regulatory, privacy, and cybersecurity requirements shall govern the access, transmission, storage, and protection of protected health information and related systems.
- Industry Standards and Cybersecurity Frameworks
- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
- NIST Special Publications (including but not limited to SP 800-53, 800-171, 800-61, and 800-63)
- Center for Internet Security (CIS) Critical Security Controls
- Multi-State Information Sharing and Analysis Center (MS-ISAC) guidance and best practices
- CISA Trusted Internet Connections (3.0) initiative
- Procurement, Technology, and Environmental Standards

- New York State Office of General Services (OGS) Procurement Guidelines
- NYS OGS Procurement Services Group – Guidelines for the Disposal and Recycling of Electronic Equipment
- Applicable County procurement policies and procedures governing technology acquisition and services
- Records, Data Governance, and Transparency
- New York State Records Retention and Disposition Schedule LGS-1
- Litigation hold and records preservation requirements
- County data classification, retention, and access control policies
- County-Level Governance and Authority
- Sullivan County Information Technology Governance Policies and Standards
- Sullivan County Data Storage, Security, and Acceptable Use Policies
- Sullivan County Legislative Resolutions governing information technology authority and procurement, including but not limited to Resolution No. 110-24
- Directives issued by the County Manager and County Legislature

Replaces & Supersedes: All policies issued prior to May 2026

Revision Dates: May 2026 - SCITS-0001.000 Approved Resolution XXX-26

- Complete ITS policy rewrite.

Issued By:
Lorne D. Green
Commissioner and Chief Information Officer
Division of Information Technology Services

Approved By:
Sullivan County Legislature
Resolution #XXX-26
Date:

[Resolution Image Placeholder Page]

Contents

Section 1: Information Technology Governance

1.00 Introduction

Sullivan County invests substantial public resources in information technology, including computer systems, network infrastructure, software, telecommunications, cloud-based services, Internet connectivity, cybersecurity tools, and the personnel and professional services necessary to support those systems. The County relies upon information technology to conduct essential government operations, including the storage, processing, transmission, and reporting of financial, administrative, personnel, geospatial, public safety, health, and other sensitive or confidential information.

County information systems and the data they contain are critical public assets. These assets must be protected from unauthorized access, misuse, disclosure, alteration, destruction, disruption, inefficiency, and waste. This responsibility has become increasingly important due to the growing frequency, sophistication, and impact of cyber threats, including phishing, malware, ransomware, credential theft, business email compromise, insider misuse, supply chain compromise, and other malicious or negligent acts.

No single technology, policy, or practice can adequately protect County information assets. Effective information security requires a coordinated system of governance, policies, standards, technical safeguards, monitoring, training, accountability, and enforcement. When these controls are properly designed, implemented, and maintained, they reduce risk and improve the County's ability to protect systems and data, support operations, comply with legal requirements, and recover from disruptive events.

The County Legislature, County Manager, Commissioners, Department Heads, and Information Technology Services all have important roles in ensuring that appropriate information technology and cybersecurity controls are established and maintained. Because technology, threat conditions, legal requirements, and business operations continue to evolve, information security must be treated as a continuous governance function rather than a one-time compliance exercise.

This handbook, together with the related policies, standards, guidelines, and procedures adopted by the County, is intended to provide a uniform framework for the governance, acceptable use, protection, and management of County information technology resources. It defines responsibilities, establishes expectations for behavior and control, describes required safeguards, and identifies consequences for noncompliance. Its purpose is to strengthen oversight of County information technology assets and support a secure, reliable, and accountable operating environment. Individual policies are designed to function as standalone documents; as such, certain requirements may be reiterated to ensure clarity, enforceability, and independent applicability.

Policy Structure Note: This document is intentionally designed as a unified compendium of Sullivan County information technology governance and cybersecurity policies. Each section and policy is written to function both as part of the comprehensive framework and as a fully independent,

standalone policy. Redundancy across sections is intentional to ensure that each policy remains complete, auditable, and enforceable when distributed or referenced individually.

Requests for exceptions to this policy must be submitted in writing, include a documented business justification and risk assessment, and be approved by the Chief Information Officer or designated authority. Approved exceptions shall be time-bound and subject to periodic review.

1.01 Responsibility and Accountability for Internal Controls

Internal controls are essential to the effective, lawful, and efficient operation of Sullivan County government. Internal controls include the policies, procedures, organizational responsibilities, technical safeguards, and oversight activities that are designed to provide reasonable assurance that County operations are functioning as intended, that assets are protected, that records are accurate, that risks are managed appropriately, and that applicable laws, regulations, and contractual obligations are met.

In the context of information technology, internal controls are intended to ensure that County systems and the information they process, store, and transmit are reliable, available when needed, appropriately secured, and protected against unauthorized access, misuse, alteration, or loss. These controls also support operational continuity, legal compliance, financial stewardship, and public trust.

The policies contained in this handbook establish the minimum standards, expectations, responsibilities, and acceptable practices required of County departments, employees, contractors, and other authorized users. Section 2, Information Technology Policy, Guidelines and Procedures, sets forth the County's minimum requirements for acceptable use, information security, data protection, and operational control. Compliance with these policies is mandatory. Each County department is responsible for ensuring that the policies are communicated, implemented, followed, and enforced within its area of responsibility.

This handbook applies to all County information technology resources, whether owned, leased, licensed, hosted, managed, or otherwise used by or on behalf of Sullivan County. This includes, but is not limited to, hardware, software, cloud services, business applications, mobile devices, telecommunications systems, electronic records, physical infrastructure, and wired and wireless networks, regardless of location. This handbook also applies to systems and services administered for the County by third parties.

Any County department may impose more restrictive standards, controls, or procedures where required by operational need, risk profile, legal obligation, grant condition, regulatory requirement, or contractual commitment, including but not limited to HIPAA, CJIS, PCI-DSS, public safety requirements, election security requirements, or other State and Federal mandates. However, no department may adopt practices that fall below the minimum standards established in this handbook unless a written exception is approved by the Chief Information Officer or by other authority expressly designated by County policy or law.

The internal controls and policies outlined in this handbook are intended to:

- Communicate responsibility for the protection of County information and technology resources;
- Establish minimum standards for the acceptable use of County-owned, County-managed, or County-connected technology resources;
- Support the secure and effective administration of County systems, services, and data;
- Reduce the risk of security incidents, service disruption, data loss, fraud, misuse, and unauthorized disclosure;
- Preserve the County's legal, operational, disciplinary, and management options in the event of misuse, compromise, or noncompliance; and
- Promote accountability, resilience, and continuity in support of County operations.

These policies and procedures apply to all County departments, but they are not intended to unilaterally alter the terms and conditions of employment, applicable law, or collective bargaining agreements. Departments shall implement these requirements in a manner consistent with all applicable personnel rules, labor obligations, legal requirements, and operational responsibilities. Nothing in this handbook shall be interpreted to supersede applicable personnel policies, collective bargaining agreements, or governing law.

These policies, guidelines, and procedures apply to all County staff and to all other persons or entities, including contractors, consultants, vendors, interns, volunteers, temporary staff, and outsourced service providers, who access, use, support, host, process, transmit, store, or manage County information or information technology resources. Where a conflict exists between this handbook and a departmental guideline, contract term, or operational practice, the more restrictive security requirement shall govern unless otherwise directed in writing by the County.

This Employee Handbook for Information Security applies to all information, regardless of form or format, and to all systems, whether manual or automated, for which Sullivan County has ownership, custody, responsibility, or administrative authority. It shall be communicated to all personnel and other authorized users who access or manage County information or systems and shall be made available for reference through appropriate County channels.

1.02 Cybersecurity Authority and Governance

Sullivan County adopts a risk-based, Zero Trust approach to cybersecurity in which no user, device, system, or network—whether internal or external—is inherently trusted. Access to County systems and data shall be continuously evaluated and granted based on verified identity, device security posture, least privilege, and business need. All systems, services, and connections shall be designed, implemented, and operated in alignment with this principle.

The Commissioner of Information Technology / Chief Information Officer (CIO) is the County's designated authority for cybersecurity and retains final operational authority over County

cybersecurity standards, controls, incident response actions, and security risk determinations, except where otherwise required by law or expressly directed by the County Manager or County Legislature. This authority shall be exercised in coordination with County leadership and in accordance with applicable law and governance structures.

The CIO is responsible for establishing, administering, and enforcing County-wide cybersecurity policies, standards, controls, and operational requirements necessary to protect County systems, networks, services, and data.

In that role, the CIO has authority to:

- Establish and issue County-wide information security standards, procedures, and technical requirements;
- Direct and coordinate the County's response to cybersecurity threats, vulnerabilities, and incidents;
- Approve, conditionally approve, or deny technologies, services, configurations, connections, and practices that affect the security, confidentiality, integrity, availability, or resilience of County systems or data;
- Require corrective action or remediation where security deficiencies, unsafe practices, or policy noncompliance are identified;
- Enforce minimum security requirements for County-operated and third-party-operated systems and services;
- Review and approve external connectivity, remote access methods, identity and access controls, and cybersecurity exceptions; and
- Take immediate action, including restricting access, isolating systems, disabling accounts, suspending services, or directing other protective measures, when necessary to protect County operations, systems, or information.

This authority is consistent with and supported by Sullivan County Legislative Resolution No. 110-24, which establishes the centralized control and jurisdiction of Information Technology Services over County software, systems, and related technology assets.

All County departments shall comply with cybersecurity directives issued by the CIO or designee, in accordance with applicable law and County governance requirements. In the event of a conflict between operational preference and cybersecurity requirements, the determination of the CIO shall govern unless otherwise directed by the County Manager, County Legislature, or applicable law.

Cybersecurity governance within the County shall be risk-based, aligned to recognized best practices, and designed to support secure service delivery, accountability, compliance, resilience, and continuity of operations.

Authoritative Interpretation

Authoritative interpretation of this policy resides solely with the Commissioner of Information Technology / Chief Information Officer (CIO), the County Manager, or designated legal authority. Informal interpretations, opinions, or statements by employees or third parties shall not be considered binding interpretations of County policy.

1.03 Organizational Security and Departmental Responsibilities

County Departments

Each County department shall establish and maintain an internal framework to support the implementation, review, and control of information security within its area of responsibility. Department Heads are responsible for ensuring that information assets under their control are appropriately managed and protected in accordance with County policy, legal requirements, and operational needs.

Each department shall ensure that appropriate processes are in place for:

- Implementing and reviewing applicable acceptable use and information security policies, standards, and procedures;
- Assigning information security and data stewardship responsibilities;
- Identifying and communicating legal, regulatory, contractual, or operational requirements affecting information security;
- Determining information sensitivity and appropriate protection levels;
- Monitoring significant changes in risk exposure, business process, legal obligation, or technology use;
- Responding to and reporting security incidents, suspected misuse, and control deficiencies;
- Ensuring that security requirements are addressed in third-party relationships, contracts, and operational practices; and
- Supporting required training, awareness, and compliance activities.

Department Heads are responsible for ensuring that all staff members are made aware of the Employee Handbook for Information Security and any related departmental requirements. Department Heads shall ensure that required acknowledgements are completed and retained in accordance with County procedure.

Information Owners

County departments are the information owners of the data, records, and systems used in support of their functions, except where law, policy, or system design assigns ownership otherwise. Information owners are responsible for determining who should have access to protected resources within their authority and what level of access is appropriate based on business need, role, and legal or regulatory requirements.

Information owners are responsible for:

- Identifying and classifying information assets within their authority;
- Defining appropriate access rights and approval processes;
- Ensuring that access privileges are consistent with job responsibilities and least privilege principles;
- Communicating legal, confidentiality, records, and disclosure requirements to Information Technology and other support personnel as necessary;
- Supporting the implementation of required safeguards for information under their control;
- Periodically reviewing access and control effectiveness; and
- Reporting material control deficiencies, risks, or incidents through appropriate channels.

Responsibility for implementing specific controls may be delegated; however, accountability for the protection of the asset remains with the designated information owner.

1.04 Information Security Officers: Roles and Responsibilities

Sullivan County maintains a decentralized operating environment in which certain departments have specialized legal, regulatory, or operational responsibilities related to information security. Designated Information Security roles may be assigned where required; however, such roles shall be limited to Management Confidential (MC) or otherwise authorized positions consistent with applicable job classifications, unless formally designated by the County.

Such roles may include, as applicable:

- The Commissioner of Information Technology / Chief Information Officer, responsible for County-wide information technology governance, cybersecurity direction, core enterprise systems, and disaster recovery oversight;
- The e911 Director of Communications, responsible for information security matters relating to dispatch systems and associated public safety operations within the scope of assigned authority;
- The EMS Coordinator or other designated official, responsible for information security matters relating to emergency medical services data and systems within the scope of assigned authority;
- The Public Health Department Director or other designated official, responsible for information security matters relating to public health information and applicable health data protections;
- The Director of Mental Health or other designated official, responsible for information security matters relating to mental health and patient care information within the scope of assigned authority; and
- The County Compliance Officer or other designated official, responsible for compliance oversight functions assigned by law, policy, or administrative structure, including HIPAA and PCI oversight where applicable.

The purpose of the Information Security Officer function is to support the secure operation of County business processes and technologies through the development, implementation, communication, and oversight of information security requirements and practices.

Information Security Officers are responsible, within their assigned areas and consistent with County-wide direction, for:

- Supporting the development, implementation, and maintenance of information security standards, procedures, and control processes;
- Providing guidance regarding security risks, vulnerabilities, threats, and compensating controls;
- Assisting departmental leadership in implementing security measures appropriate to business need and legal requirement;
- Supporting or facilitating security awareness and training activities;
- Reporting, investigating, or coordinating response to suspected or confirmed security incidents as appropriate;
- Participating in continuity, disaster recovery, and resilience planning;
- Coordinating with Information Technology, compliance, legal, management, and law enforcement entities as needed;
- Remaining informed regarding applicable laws, regulations, standards, and emerging risks affecting County information assets; and
- Maintaining an appropriate level of professional knowledge and proficiency.

While departmental Information Security Officers may have operational responsibilities within their areas, all such roles operate under the authority and direction of the CIO for purposes of County-wide cybersecurity governance, incident response coordination, minimum control standards, and enforcement of County security requirements.

Information Security Officers shall coordinate security program activities and reporting processes as needed in support of County policy and other security initiatives. They shall also ensure that alleged information security violations are appropriately referred, documented, escalated, and investigated in accordance with County procedure and applicable law.

Department Security Administrators

Where designated, Department Security Administrators or equivalent staff shall work closely with the CIO, Information Security Officers, Information Technology personnel, and departmental support staff. These individuals may be responsible for administering security tools, managing access requests, implementing technical controls, reviewing security practices, analyzing security events, supporting audits, documenting exceptions, and assisting with response activities.

Where such functions exist, they shall include responsibility for administering account and access control processes, including the assignment, change, removal, review, logging, escalation, and reporting of access rights, privileged access, emergency access, and related exceptions.

Where no formal Security Administration function exists within a department, the individuals or teams performing those duties shall adhere to the requirements of this handbook and any related County standards or procedures.

County Employees

All County employees are responsible for protecting County information and technology resources entrusted to them or accessible through their work. This responsibility includes, but is not limited to, safeguarding credentials, using County systems only as authorized, complying with security policies and procedures, reporting suspected security incidents or misuse, and cooperating with security and compliance requirements.

County employees are expected to adhere to this handbook and all related policies, standards, and procedures issued by the County.

Non-County Personnel

Individuals who work with or on behalf of the County, including contractors, consultants, vendors, volunteers, interns, temporary staff, service providers, and other non-County personnel, are subject to this handbook to the extent that they access, use, support, host, process, transmit, store, or manage County information or County technology resources. Appropriate contractual, administrative, and technical controls shall be used to ensure compliance where applicable.

Information Technology Services

Information Technology Services is responsible for the administration, support, maintenance, protection, and continuous improvement of the County's shared technology environment, including core infrastructure, enterprise systems, identity and access management systems, data and communications networks, wireless services, cybersecurity tools, backup systems, disaster recovery capabilities, and related support services.

Information Technology Services shall support and enforce this handbook and shall provide the technical, procedural, and administrative resources necessary to maintain a level of information security consistent with County requirements, operational need, and risk.

Information Technology Services has responsibility for:

- Identifying and implementing technical safeguards required to support County business and security requirements;
- Supporting the protection of information assets based on assigned ownership, classification, and risk;
- Participating in the selection, implementation, and maintenance of cost-effective security controls and technologies;

- Defining and enforcing technical access requirements for systems, applications, networks, devices, and services under County control;
- Supporting secure backup, off-site protection, restoration, continuity, and disaster recovery functions;
- Monitoring systems, vulnerabilities, and security events where feasible;
- Supporting policy implementation, user education, and operational compliance; and
- Taking protective action as necessary to preserve the security, integrity, or availability of County systems and data.

Information Technology personnel designated to implement and administer these requirements are responsible for technical execution and operational support. Department Heads, supervisors, and authorized users remain responsible for compliance within their respective areas of authority.

1.05 Security and Accountability

All County information, regardless of form, format, or storage method, that is created, received, maintained, transmitted, processed, or used in support of County business is a County asset and shall be used and protected accordingly. County information shall be protected throughout its lifecycle, from creation or acquisition through use, storage, retention, disclosure, archival, and authorized disposition.

Information shall be maintained in a secure, accurate, reliable, and accessible manner appropriate to its business value, sensitivity, legal status, operational importance, and risk of loss or misuse. Information shall be classified and protected in accordance with applicable County requirements, legal obligations, and recognized security best practices.

The security of County information and the systems that support it is a shared responsibility. All authorized users are required to protect County information in a manner that supports confidentiality, integrity, availability, accountability, and privacy, as applicable. These protections shall be achieved through a combination of administrative, technical, and physical controls.

Information security management shall support the appropriate sharing and use of information while ensuring that such sharing occurs in a controlled, lawful, and secure manner. County-designated personnel shall ensure that safeguards are implemented and maintained to preserve the security objectives of County information and the systems on which it resides.

Individual Accountability

Individual accountability is a foundational principle of County information security. Access to County systems, applications, networks, and information resources shall be attributable to a specific authorized individual or to an approved non-person account where operationally necessary and appropriately controlled.

Where credentials are suspected to be compromised, shared, or misused, Information Technology Services retains authority to immediately disable access, reset credentials, or impose protective controls without prior notice.

Accordingly:

- Access to County systems and information resources shall be provided through individually assigned unique identifiers or other approved authentication mechanisms;
- Individuals shall access only those systems, data, and functions for which they are authorized and for which a legitimate business need exists;
- Authentication information, including passwords, passphrases, tokens, codes, and similar credentials, shall be treated as confidential and shall not be disclosed or improperly stored;
- Each user is responsible for all activity performed using his or her credentials and shall take reasonable steps to protect those credentials from unauthorized use;
- Shared credentials are prohibited unless expressly approved, documented, and controlled for operational necessity;
- Credentials shall not be posted, written in unsecured locations, transmitted insecurely, or otherwise exposed to unauthorized persons.

Additional requirements relating to authentication, account management, and credential practices are set forth in applicable Information Technology policies, standards, and procedures.

1.06 Policy Monitoring and Enforcement

County technology systems, services, networks, accounts, devices, and records are the property of Sullivan County or are operated on its behalf for County business purposes. Subject to applicable law, policy, due process, and operational necessity, the County reserves the right to monitor, review, retrieve, preserve, and disclose information relating to the use of its systems, services, devices, accounts, communications, and records for legitimate governmental, security, operational, legal, audit, investigatory, and compliance purposes.

County systems, including mobile devices and network-connected equipment, may utilize monitoring, logging, and location-based services for security, operational, and asset management purposes. Users shall not disable, circumvent, or interfere with such controls where implemented.

Although the County does not continuously monitor all user activity or routinely review the content of communications, information may be accessed, reviewed, or preserved in the normal course of system administration, troubleshooting, security monitoring, records retention, legal process, investigation, or incident response.

Backup or archived copies of communications and other records may exist despite end-user deletion. Such retention supports business continuity, records management, legal compliance, system reliability, and recovery from data loss or system failure.

If the County discovers, or has reason to suspect, activity that does not comply with applicable law, policy, contract, or operational requirements, relevant records may be retrieved, preserved, reviewed, and used in accordance with due process and applicable procedures. Where appropriate and practicable, reasonable efforts may be made to notify affected personnel; however, advance notice may not be possible or appropriate in all cases.

All monitoring and enforcement activities shall be conducted in accordance with applicable personnel policies, collective bargaining agreements, and legal requirements.

Users shall exercise caution when transmitting confidential, sensitive, or restricted information through electronic means. Communications concerning County business may be subject to records retention, disclosure, audit, litigation hold, subpoena, e-discovery, or Freedom of Information Law (FOIL) requirements. Users shall communicate in a manner that is accurate, professional, lawful, and appropriate to the public nature of government operations.

1.07 Reporting Misuse or Security Concerns

Any suspected misuse of County technology resources, policy violation, unauthorized access, phishing attempt, data exposure, loss of equipment, or other security concern shall be reported immediately to the employee's supervisor, Department Head, Information Technology Services, or the Chief Information Officer, as applicable. Offensive, suspicious, or potentially malicious messages or communications should not be forwarded, deleted, or replied to unless directed by Information Technology or other authorized personnel as part of an investigation or response.

The County shall maintain appropriate reporting channels for the prompt escalation of information security concerns. Reporting and follow-up actions shall be handled in a manner consistent with applicable personnel policies, confidentiality requirements, and legal obligations, and shall be conducted in a fair and appropriate manner.

Disclaimer

Nothing in this policy shall be construed to limit, waive, or supersede any rights, protections, or obligations of Sullivan County under applicable federal, state, or local law.

Users are responsible for the content they create, access, transmit, store, or disseminate using County systems and technology resources, subject to applicable law, County policy, and the scope of their authorized duties.

To the extent permitted by law, Sullivan County shall not be liable for any direct, indirect, incidental, or consequential damages arising from the improper, unauthorized, or unlawful use of County technology resources, including voice, data, or information systems.

The County shall not be responsible for third-party claims, demands, or damages resulting from the unauthorized, unlawful, or improper use of County systems or information by any user.

1.08 Failure to Comply

Violations of this handbook or any related Information Security Policy may be treated as misconduct and shall be addressed in accordance with established County procedures, applicable law, personnel rules, and contractual obligations.

Sanctions for noncompliance may include, but are not limited to:

- Temporary or permanent revocation of access to County systems, services, or resources;
- Required corrective action or retraining;
- Administrative or disciplinary action;
- Termination of employment or contractual relationship, where applicable; and
- Referral for civil, regulatory, or criminal action as appropriate.

Each County department is responsible for ensuring that staff understand and comply with applicable acceptable use and information security requirements. Users are advised that the use of County-owned equipment, County accounts, County systems, and personal devices connected to County resources may be subject to monitoring, logging, restriction, or review for legitimate business, legal, operational, and security purposes.

All enforcement and corrective actions arising from non-compliance with this handbook shall be administered in accordance with applicable personnel policies, collective bargaining agreements, and legal requirements.

1.09 Operational Controls and Procedures

Implementation of the controls described in this section shall be coordinated with departmental operations and carried out in accordance with applicable governance, legal, and operational requirements.

Computer Hardware, Software, and Data Inventories

The County shall maintain an inventory of hardware, software, and other technology assets acquired through or managed by Information Technology Services. Inventory records shall be sufficiently detailed to support operational support, accountability, lifecycle management, licensing compliance, warranty management, incident response, recovery planning, replacement planning, and audit needs.

Hardware inventory records should include, as applicable, device description, manufacturer, model, serial number, asset tag, assigned user, physical location, purchase or lease information, acquisition date, support status, replacement value, warranty information, and maintenance or service plan data.

Software inventory records should include, as applicable, product name, version, licensing information, installation location, assigned system or user, acquisition information, renewal terms, and maintenance or support information.

Departments shall cooperate with Information Technology Services in maintaining complete and accurate inventories of technology assets under County control. Implementation of these controls shall be coordinated with departmental operations and carried out in accordance with applicable governance, legal, and operational requirements.

Contracts for IT Services

Sullivan County relies on third parties to provide certain information technology products and services. To protect the County's interests and reduce operational, legal, financial, and cybersecurity risk, major technology services and projects shall be governed by appropriate procurement documentation and written agreements, including Statements of Work where applicable.

Technology procurements shall follow County purchasing requirements and applicable legal and policy requirements. As appropriate, solicitations and contracts should address scope, term, deliverables, performance expectations, roles and responsibilities, security requirements, access controls, incident notification, audit rights, confidentiality, data ownership, records obligations, compliance requirements, billing, support, change management, and other conditions necessary to protect the County's interests.

No technology solution, system, service, or external connection that stores, processes, transmits, or provides access to County data shall be implemented without review and approval by the CIO or designee for cybersecurity and architectural compliance.

Malware, Ransomware, and Endpoint Protection

Sullivan County shall maintain endpoint and system protection measures designed to prevent, detect, respond to, and recover from malware, ransomware, malicious code, and related threats. These controls may include endpoint protection, endpoint detection and response, centralized alerting, behavioral analytics, signature-based detection, application controls, isolation capability, and other safeguards deemed appropriate by Information Technology Services.

Security tools shall be maintained in accordance with vendor guidance and County requirements, including timely updates of signatures, agents, rules, engines, or related protective components. Systems lacking current protection may be restricted, isolated, remediated, or removed from service where necessary to reduce risk.

Users shall not disable, tamper with, bypass, or interfere with County security software or protective controls unless expressly authorized by Information Technology Services.

Patch and Vulnerability Management

Sullivan County shall maintain a patch and vulnerability management process to reduce risk arising from known software, firmware, operating system, and application vulnerabilities.

Security updates and patches shall be applied according to risk and severity, operational feasibility, and vendor guidance. Critical vulnerabilities shall be remediated as rapidly as practicable and on an expedited basis where active exploitation is known or reasonably suspected. Other updates shall be applied within established maintenance cycles appropriate to the system, service, and associated risk.

Where feasible, vulnerability monitoring and remediation shall be supported through automated tools, testing procedures, change control practices, and validation processes. Application and system updates shall be tested as appropriate before implementation in production environments, based on operational criticality and risk.

Access Controls

Access controls determine the level and type of protection appropriate for systems, facilities, services, and information resources, and they govern who may access those resources and under what conditions. Access shall be granted only to the extent necessary for authorized users to perform their assigned duties and shall be based on business need, role, risk, and least privilege principles.

The County shall maintain procedures for granting, changing, reviewing, and terminating access rights. Such procedures shall define approval authority, technical implementation requirements, review expectations, privileged access handling, and termination timelines. Accounts for separated personnel, retired personnel, inactive users, or others no longer requiring access shall be disabled or removed in a timely manner.

Each authorized user shall be assigned a unique account or other approved authentication method to support accountability. Access shall be limited to the systems, applications, functions, and data necessary to perform assigned duties.

The County adopts a security approach under which users, devices, and connections are not trusted solely because they are internal to the network. Access decisions may take into account identity, authentication strength, device status, location, risk indicators, and system sensitivity. Additional requirements for identity and access management are set forth in applicable County policy.

Authentication and Password Requirements

Authentication controls shall be designed to reduce the risk of unauthorized access and compromise. County systems shall enforce modern authentication standards to the greatest extent feasible.

Passwords or passphrases shall meet minimum County requirements for length, strength, and screening against commonly used or compromised values. Multi-factor authentication shall be required for remote access, privileged access, cloud services where feasible, and other use cases designated by Information Technology Services.

Authentication requirements shall be established and updated by County policy and technical standard rather than fixed solely in this handbook so that they may evolve with current threats and best practices.

Wireless Networks

Wireless networks present risks similar to, and in some respects greater than, wired networks because wireless signals may extend beyond physical building boundaries and may be subject to interception, misuse, unauthorized access, and service disruption if not properly secured.

Wireless infrastructure shall be designed, deployed, and managed in a manner that supports secure coverage, strong authentication, encryption, segmentation, monitoring, and risk-appropriate control. Wireless access points, service set identifiers, and related configurations shall be managed by Information Technology Services or by other authorized personnel under County standards.

Unauthorized wireless devices, hotspots, or access points connected to County systems are prohibited unless approved by Information Technology Services.

Firewalls and Network Protection

Connections to the Internet and to external networks increase the risk of unauthorized access, attack, misuse, and disruption. Sullivan County shall maintain firewalls, filtering, segmentation, logging, and other network protection mechanisms to manage and restrict traffic based on approved rules, security requirements, and business need.

Firewall and related network security configurations shall be administered in accordance with County standards and shall support protection, monitoring, auditing, and incident response. External network connections and exceptions shall be subject to review and approval by the CIO or designee.

Physical Controls

Physical security controls shall be used to protect County technology facilities, devices, infrastructure, and information assets from unauthorized access, damage, loss, theft, tampering, environmental hazard, and operational interruption.

Such controls may include locked facilities, restricted access, surveillance, environmental monitoring, fire suppression, water detection, power protection, and related safeguards appropriate to the location and criticality of the resource.

Access to County data centers, network rooms, communications closets, and other sensitive technology spaces shall be restricted to authorized personnel and approved service providers with a legitimate business need.

1.10 Service Continuity and Disaster Recovery

Data Backups

The County shall maintain backup processes sufficient to support the recovery of critical systems and data in the event of loss, corruption, encryption, deletion, service failure, or other disruption. Backup practices shall be appropriate to the system, data classification, recovery requirement, legal obligation, and operational need.

Backup processes should include, as applicable:

- Regular backup of critical data and systems;
- Verification that backups completed successfully;
- Secure storage of backup data, including off-site or logically separated protection where appropriate;
- Periodic validation that backed-up data can be restored; and
- Protective measures to reduce the risk that backup data can be altered, deleted, or encrypted by unauthorized actors.

Where feasible, backup architecture should support resilience against ransomware and other destructive events through methods such as immutability, segmentation, retention control, and offline or otherwise protected recovery capability.

Disaster Recovery Planning

Disaster recovery is the process by which County technology services are restored following a disruptive event, whether caused by cyber incident, system failure, natural disaster, utility interruption, equipment failure, human error, or other cause.

The County shall maintain disaster recovery and related continuity planning appropriate to the size, complexity, and operational dependence of its information systems. Such planning shall address, as applicable, communication, system prioritization, recovery sequencing, restoration responsibilities, alternate processing capability, dependencies, and testing.

Critical systems shall be identified and recovery objectives established based on business need, legal requirement, and operational impact. Disaster recovery capabilities shall be reviewed and tested periodically as determined by Information Technology Services and County management.

1.11 Security Awareness, Training, and Testing

Sullivan County shall maintain a security awareness and training program appropriate to the County's size, risk profile, operational needs, and legal obligations. Because users are frequently targeted through phishing, social engineering, credential theft, and related attacks, user awareness is an essential component of the County's internal control environment.

All users who access County systems or data shall complete required security awareness training annually per New York State law. Additional training may be required for high-risk roles, privileged users, and personnel with specialized responsibilities.

Training and awareness activities may include web-based training, policy acknowledgement, periodic reminders, phishing simulations, role-based instruction, notices regarding emerging threats, and other educational measures designed to improve the County's security posture.

Departments are responsible for supporting staff completion of required training. Failure to complete mandatory training may result in restriction or suspension of access.

1.12 Compliance Requirements and Financial Controls

Sullivan County is subject to a range of legal, regulatory, contractual, and operational requirements relating to the use, disclosure, retention, security, and management of information. These may include, but are not limited to, CJIS, HIPAA, PCI-DSS, records retention requirements, public records laws, privacy laws, grant conditions, audit standards, and other State or Federal obligations.

County departments shall identify and comply with those requirements applicable to the information, systems, and operations under their control. Information Technology Services, compliance personnel, management, and legal counsel shall work cooperatively, as appropriate, to support compliance.

Because external standards and regulatory requirements change over time, detailed technical or regulatory requirements may be maintained by reference, appendix, standard, or procedure rather than fully reproduced in this handbook.

Financial transaction controls, online banking practices, payment processing controls, and related financial responsibilities shall remain under the authority of the departments charged with those duties, subject to applicable law, policy, and internal control requirements. Where County networks or systems are used in support of such activities, Information Technology Services shall provide technical safeguards consistent with its role, but departmental ownership of process and compliance responsibilities shall remain as otherwise assigned.

1.13 IT Security Fundamentals

Two foundational concepts that inform County information security are confidentiality, integrity, and availability, and the use of multiple layers of control to reduce risk.

Confidentiality, Integrity, and Availability

Confidentiality refers to protecting information from unauthorized access, use, or disclosure.

Integrity refers to protecting information and systems from unauthorized modification, destruction, or corruption and ensuring that data remains accurate, complete, and trustworthy.

Availability refers to ensuring that information and systems are accessible and usable when needed for authorized County purposes.

These principles guide the design, implementation, and evaluation of County information security controls.

Defense in Depth

Defense in depth is the practice of using multiple layers of physical, administrative, and technical safeguards to protect data, systems, and services. Because no single control is sufficient to prevent all threats, the County relies on overlapping controls, monitoring, user awareness, access restrictions, backup practices, incident response capabilities, and other measures to reduce the likelihood and impact of security failures.

A layered security approach improves the County’s ability to prevent, detect, contain, respond to, and recover from threats affecting County operations and information assets.

Section 2: Information Technology Policy, Guidelines and Procedures

The policies, guidelines, standards, and procedures set forth in the following sections establish the minimum requirements, responsibilities, ethical expectations, and acceptable practices necessary to protect Sullivan County information, systems, and technology resources, and to maintain a secure, reliable, and compliant operating environment.

These requirements are intended to support the County's information security objectives, including the protection of confidentiality, integrity, availability, accountability, and privacy of County information, as well as the continuity of County operations and compliance with applicable legal, regulatory, and contractual obligations.

These policies, guidelines, standards, and procedures apply to all County departments, elected officials, employees, contractors, consultants, vendors, volunteers, interns, and any other individuals or entities who access, use, support, host, process, transmit, store, or manage County information or County information technology resources, whether such access occurs on County-owned systems or through external or third-party systems connected to or used on behalf of the County.

All users of County information technology resources are expected to comply with these requirements as a condition of access. Department Heads are responsible for ensuring that these requirements are communicated, understood, and enforced within their respective departments.

Where a conflict exists between these policies and a departmental policy, operational practice, contractual provision, or external requirement, the **more restrictive security requirement shall govern**, unless otherwise approved in writing by the Chief Information Officer (CIO) or required by law.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, shall have authority to interpret, implement, and enforce these policies and to issue supporting standards, procedures, and technical controls necessary to ensure compliance and to address evolving risks, threats, and operational requirements.

Compliance with these policies, guidelines, standards, and procedures is mandatory. Failure to comply may result in restriction or revocation of access to County systems, disciplinary action, termination of employment or contractual relationship, and/or referral for legal or regulatory action, as appropriate.

Any suspected or actual misuse of County information technology resources, policy violation, unauthorized access, data exposure, or other security concern shall be reported immediately to the user's supervisor, Department Head, Information Technology Services, or the CIO. Reports may also be submitted through designated IT security reporting channels as established by the County.

Policy numbering follows a domain-based structure. The first two digits represent the control domain, the second two digits represent the specific policy within that domain, and the decimal suffix

represents the version of the policy. Version numbers are incremented upon formal revision and reissuance. Policy numbering may reflect version history and may not be sequential.

Nothing in this section shall be interpreted to limit the authority of the County to monitor, audit, restrict, or control the use of its information technology resources in accordance with applicable law, policy, and operational necessity.

Section 3 — Identity and Access Management (3000 Series)

SCITS-3005.001 – Identity and Access Management Overview

Title	Number
SCITS-3005.001 – Identity and Access Management Overview	SCITS-3005.001

Creation Date: May 2026

Modified Date:

Purpose

The purpose of this policy is to establish requirements for the creation, management, use, and control of user identities and access credentials used to access Sullivan County information technology resources.

Proper identity and access management is essential to ensuring that only authorized individuals are granted access to County systems, applications, and data, and that such access is appropriately controlled, monitored, and revoked when no longer required.

Scope

This policy applies to:

- All Sullivan County information systems, applications, networks, and technology resources;
- All user identities, including network accounts, application accounts, and other authentication credentials;
- All employees, elected officials, contractors, consultants, vendors, interns, volunteers, and other authorized users; and
- All systems that authenticate or authorize access to County resources, whether managed internally or by third parties.

Access to County systems is a privilege, not a right, and shall be granted only where a valid business need and authorized relationship with the County exists.

General Policy

All access to Sullivan County information technology resources shall be provisioned through unique, individually assigned user identities, typically in the form of a centralized network account (e.g., Active Directory or its successor), and may include application-specific accounts where required.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has authority over identity and access management, including account provisioning, authentication standards, access control enforcement, and lifecycle management.

User accounts shall be created only upon receipt of an authorized request and verification of eligibility. Valid relationships include, but are not limited to:

- County employees;
- Elected officials;
- Interns and temporary staff;
- Contractors, consultants, and vendors; and
- Other individuals with an approved and documented business need.

All access requests must be submitted through approved processes and must include appropriate authorization from the Department Head or designated authority. Information Technology Services shall verify eligibility and ensure that access is appropriate to the user's role and responsibilities.

Account Provisioning and Structure

Each authorized user shall be assigned a unique identifier (Network ID) that is attributable to that individual. Account naming conventions may follow standardized formats established by Information Technology Services; however, naming conventions may be modified as necessary to ensure uniqueness, security, and operational consistency.

Where required, users may also be assigned application-specific accounts or role-based access credentials consistent with system requirements.

Shared or generic accounts are prohibited unless explicitly approved for operational necessity and appropriately controlled.

Authentication and Credential Security

User credentials, including passwords, passphrases, tokens, or other authentication mechanisms, must be protected at all times.

Users are prohibited from:

- Sharing credentials with any other individual;
- Using another person's credentials;
- Storing credentials in an insecure manner; or
- Attempting to obtain unauthorized access to another user's account.

Authentication requirements, including password standards, multi-factor authentication, and credential lifecycle requirements, shall be defined and enforced by Information Technology Services in accordance with County policy and current security best practices.

Users are responsible for all activity conducted under their assigned credentials and must take reasonable precautions to prevent unauthorized use.

Account Usage and Responsibility

User accounts shall be used only by the individual to whom they are assigned and only for authorized County business purposes.

Users shall access only those systems, applications, and data necessary to perform their assigned duties.

Any suspected compromise of credentials or unauthorized access must be reported immediately to Information Technology Services.

Account Lifecycle Management

User accounts shall be managed throughout their lifecycle, including creation, modification, suspension, and removal.

Accounts shall be:

- Created upon authorized request and verification of eligibility;
- Modified as necessary to reflect changes in role or responsibilities;
- Disabled promptly upon termination of employment, contract, or authorized relationship; and
- Periodically reviewed to ensure continued necessity and appropriateness of access.

Inactive accounts shall be automatically disabled after a defined period of inactivity as determined by Information Technology Services. Accounts that remain inactive beyond an additional defined period may be permanently removed.

Specific inactivity thresholds and lifecycle timelines shall be established and maintained by Information Technology Services to reflect current operational and security requirements.

Monitoring and Enforcement

Sullivan County reserves the right, subject to applicable law, to monitor and audit user account activity to ensure compliance with this policy and to detect unauthorized access or misuse.

Accounts found to be in violation of this policy may be suspended, restricted, or terminated.

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contractual relationship, and/or legal action where applicable.

Reporting Requirements

Any suspected misuse of accounts, credential compromise, unauthorized access, or policy violation shall be reported immediately to a supervisor, Department Head, Information Technology Services, or the Chief Information Officer (CIO).

Disclaimer

Sullivan County assumes no liability for damages arising from unauthorized use of user accounts where such use results from failure to comply with this policy, except as otherwise required by law.

SCITS-3010.001 Policy – Network ID Maintenance

Title	Number
Network ID Maintenance	SCITS-3010.001
Creation Date: May 2026	
Modified Date:	

Purpose

The purpose of this policy is to establish a standardized, controlled process for the creation, modification, and removal of network (voice or data) and application access for employees, contractors, and other authorized agents acting on behalf of Sullivan County. This policy ensures that access to County systems is provisioned, managed, and revoked in a secure, auditable, and timely manner consistent with business need and applicable security requirements.

Scope

This policy applies to all Sullivan County departments without exception. All requests to add, change, or remove access to County network resources, systems, telecommunications services, or applications shall be submitted and processed in accordance with this policy.

General Policy

1. Access Request and Authorization

All access provisioning actions—including the addition, modification, or removal of access—shall be initiated through an approved **New User Request Form**.

Each request shall:

- Specify the action required (add, change, or delete);
- Identify all required network, application, and telecommunications access; and
- Include sufficient detail to support appropriate access provisioning based on business need.

Requests must be submitted by a Department Head or an authorized designee.
Requests submitted via telephone, email, or other informal methods shall not be accepted or processed.

2. Identity Lifecycle Management

All user accounts shall be managed throughout their lifecycle, including provisioning (onboarding), modification (role changes), and deprovisioning (separation or end of engagement), using approved and documented processes to ensure accuracy, accountability, and auditability.

Departments shall submit all user role changes, transfers, and reassignments in a timely manner to ensure appropriate access is maintained.

3. Timely Deprovisioning

User access shall be disabled or removed promptly upon employee separation, termination, contract expiration, or reassignment.
In all cases, access removal shall occur as soon as practicable and no later than the end of the business day of notification.

4. Least Privilege and Access Control

Access to County systems shall be granted based on the principle of **least privilege**, limiting access strictly to the minimum necessary to perform assigned job functions.

Information Technology Services (ITS) shall review requested access and may modify or restrict access to align with security requirements, system capabilities, and County policy.

5. Unique User Identification

All users shall be assigned a unique network identity.
Shared or generic accounts are prohibited unless explicitly approved by Information Technology Services and appropriately controlled, documented, and monitored.

6. Authentication and Security Requirements

Access to County systems shall comply with applicable authentication and security standards, including the use of multi-factor authentication (MFA) where required.
All access shall align with County cybersecurity policies and applicable regulatory requirements.

7. Auditability and Record Retention

All access requests, approvals, and provisioning actions shall be documented and retained in accordance with County record retention requirements.
Such records shall be maintained in a manner that supports audit, compliance review, and incident investigation.

8. Periodic Access Review

Departments, in coordination with Information Technology Services, shall periodically review user access to ensure that permissions remain appropriate and aligned with current job responsibilities. Access that is no longer required shall be promptly removed.

9. Enforcement Authority

Information Technology Services reserves the authority to validate, modify, restrict, or deny requested access where it does not align with business need, security requirements, or County policy.
ITS may suspend or revoke access where a risk to County systems or data is identified.

SCITS-3020.001 Policy – Authentication and Password Management

Title	Number
Authentication and Password Management	**SCITS-3020.001**
Creation Date: **May 2026**	
Modified Date:	

Purpose

Authentication credentials, including passwords and passphrases, are a critical component of Sullivan County's information security program. These credentials serve to verify the identity of users and control access to County systems, applications, and data.

Improper construction, handling, or protection of credentials significantly increases the risk of unauthorized access, data compromise, and system disruption.

The purpose of this policy is to establish requirements for the creation, use, protection, and management of authentication credentials to ensure secure access to County technology resources.

Scope

This policy applies to:

- All Sullivan County employees, elected officials, contractors, consultants, vendors, interns, and other authorized users;
- All systems, applications, and devices requiring authentication credentials; and
- All forms of authentication, including passwords, passphrases, PINs, and other credential-based access methods.

General Policy

All users must use secure authentication credentials that meet County-defined standards. Authentication requirements shall be established and enforced by Information Technology Services under the authority of the Commissioner of Information Technology / Chief Information Officer (CIO), or designee.

Modern best practices favor the use of **passphrases** over traditional complex passwords. Users are strongly encouraged to create long, memorable passphrases that are resistant to guessing and automated attacks.

Authentication controls, including complexity, length, reuse restrictions, and lifecycle requirements, may vary based on system sensitivity, risk level, and regulatory requirements, as determined by Information Technology Services.

Credential Construction Requirements

All authentication credentials must meet the following minimum requirements:

- Passwords shall meet minimum length and complexity requirements as defined by current County standards (minimum 12 characters unless otherwise approved by ITS);
- Use of a passphrase or combination of words that is not easily guessable;
- Avoidance of common words, predictable patterns, or publicly available personal information (e.g., names, birthdays, addresses);
- Sufficient complexity to resist automated and manual guessing attempts.

Users are encouraged to:

- Use passphrases consisting of multiple unrelated words;
- Include a mix of character types (letters, numbers, and symbols) where appropriate; and
- Create credentials that are easy to remember but difficult for others to guess.

Information Technology Services may enforce additional requirements for certain systems based on security or compliance needs.

Credential Protection and Use

Authentication credentials are confidential and must be protected at all times.

Users are prohibited from:

- Sharing credentials with any individual, including supervisors, coworkers, or Information Technology personnel;
- Using another individual’s credentials;
- Storing credentials in an unsecured manner;
- Transmitting credentials over unencrypted or untrusted channels; or
- Allowing applications or systems to store credentials insecurely.

Users are responsible for all activity conducted under their credentials and must take reasonable precautions to prevent unauthorized access.

Use of password management tools approved by Information Technology Services is permitted and encouraged.

Credential Lifecycle and Reuse

Credential lifecycle requirements, including expiration, reuse restrictions, and minimum age requirements, shall be defined and enforced by Information Technology Services based on current security standards and operational needs.

Credentials shall not be reused across systems where such reuse would introduce security risk.

Users may be required to change credentials:

- Upon initial account setup;
- Following a suspected or confirmed compromise;
- When directed by Information Technology Services; or
- As required by system-specific security policies.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is required for access to designated Sullivan County systems, applications, and services, as determined by Information Technology Services based on risk, sensitivity, and regulatory requirements.

Sullivan County utilizes a centrally managed MFA solution, currently **DUO Security**, or its successor as designated by Information Technology Services.

All users required to utilize MFA shall authenticate using at least two factors, which may include:

- Something the user knows (e.g., password or passphrase);
- Something the user has (e.g., hardware token or registered device); and/or
- Something the user is (e.g., biometric verification, where applicable).

Approved MFA methods may include:

- County-issued hardware tokens;
- DUO Mobile application push notifications;
- Telephone call verification; and
- SMS/text-based verification, where permitted.

Sullivan County shall issue a hardware token or equivalent authentication method to all users requiring MFA to ensure access is maintained regardless of personal device availability.

Users are responsible for maintaining control of their MFA authentication method(s) and must not share, transfer, or allow unauthorized use of such devices or credentials.

Loss, theft, or compromise of an MFA device or method must be reported immediately to Information Technology Services.

Information Technology Services reserves the right to restrict, modify, or disable MFA methods based on security risk, regulatory requirements, or operational considerations.

Users shall not attempt to bypass, disable, or otherwise circumvent MFA controls.

Credential Compromise and Incident Response

If a user knows or suspects that their credentials have been compromised, they must:

- Immediately change their credentials; and
- Notify Information Technology Services without delay.

Information Technology Services may reset credentials, revoke access, or take additional protective actions as necessary to secure County systems.

Storage and Transmission of Credentials

Credentials shall not be written, printed, or stored in any physical or electronic location that is accessible to unauthorized individuals, including desks, workstations, or unsecured documents.

Credentials shall not be:

- Written down or stored in plain text;
- Stored in unsecured electronic files or systems;
- Transmitted via unencrypted email, messaging, or other insecure methods; or
- Embedded in scripts, applications, or systems without appropriate security controls.

Where storage of credentials is operationally necessary, it shall be performed using secure, encrypted methods approved by Information Technology Services.

The use of password managers or credential storage tools must be limited to solutions approved by Information Technology Services.

Monitoring and Security Testing

Sullivan County reserves the right, subject to applicable law, to conduct security monitoring, auditing, and testing of authentication controls, including password strength assessments and vulnerability testing.

If a credential is determined to be weak or compromised, the user will be required to change it immediately.

Password Reset and Account Recovery

Users who forget their credentials or experience account lockout must follow approved account recovery procedures.

Password resets shall be performed through authorized methods, which may include:

- Verified identity validation through the IT Help Desk; or
- Approved self-service password reset tools, where available.

Information Technology Services shall verify user identity prior to resetting credentials.

Enforcement

Failure to comply with this policy may result in:

- Suspension or revocation of access;
- Disciplinary action, up to and including termination; and/or
- Legal action where applicable.

Disclaimer

Sullivan County assumes no liability for damages resulting from unauthorized access due to failure to comply with this policy, except as otherwise required by law.

SCITS-3030.003 Identification/Access Card and Multi-Factor Authentication Policy

Title	Number
Identification/Access Card and Multi-Factor Authentication (MFA) Policy	**SCITS-3030.003**
Creation Date: **September 2018**	
Modified Date: **April 2026**	

Purpose

It is the policy of the County of Sullivan (County) to establish and maintain a secure process for issuing, managing, and controlling Identification/Access Cards and multi-factor authentication (MFA) methods used to access County facilities, systems, and data.

Identification/Access Cards and MFA methods are components of the County's identity and access management framework and are used to support the verification of authorized individuals. These controls are intended to enhance security but shall not be relied upon as sole indicators of trust. Access to County facilities, systems, and information remains subject to verification, monitoring, and enforcement in accordance with County cybersecurity policies.

Multi-factor authentication (MFA) may include hardware tokens, software-based authenticators, or other authentication mechanisms approved by Information Technology Services (ITS). MFA requirements shall be enforced based on system sensitivity, risk, and regulatory requirements as determined by ITS.

Scope

This operating procedure applies to all full-time, part-time employees, volunteers, temporary contract employees, interns and visitors.

Procedure

A. Building Access

1. The main entrance to the County is open to the public Monday-Friday, 9:00 AM – 5:00 PM. You will need a card to gain entry during all other times.

2. In order to enter a door using a card, look for a small, black, rectangular card reader next to the door. This reader has one (1) red light on the face of the unit. Place your

card within four inches of the reader to activate it. The reader will emit a beep. If your card has been programmed to allow access through that door at that time, a green light will appear on the reader's face. Once the green light turns on, the door will unlock for five (5) seconds.

3. Employees should not open the door for others that do not have their own card, but rather direct the person to the Sheriff's Office Main Lobby Security Desk for assistance.

B. Eligibility - The following individuals are eligible to receive identification cards and/or MFA methods *(MFA methods are issued only after an approved user account has been provisioned in accordance with County identity and access management procedures.)*:

1. Elected and appointed County officials;

2. Employees officially employed by the County and currently carried on the County payroll;

3. Individuals designated as a Contractor-Special Status and currently carried on the County payroll;

4. Individuals providing volunteer or special services who are officially designated by their department head to receive a temporary card.

C. Displaying Cards

1. All employees and designated individuals must wear cards with the front of the card visible or have the card available if the employee wears a uniform that displays their name when on duty, providing services, or accessing County facilities.

D. Maintenance and Control

1. All employees are required to have an access card or they will not be allowed through the secured common areas of the buildings.

2. Please note that the identification cards and MFA methods remain the property of the County.

3. Do not prop open doors as this will activate a security alert.

4. Do not punch holes in the card, attach or affix any pins or decorations to the card, bend the card, or wash the card or token as it may be rendered inoperable.

5. Identification cards and MFA methods shall be safeguarded at all times and must not be left unattended, stored insecurely, or handled in a manner that increases the risk of loss, theft, or misuse.

6. Identification cards and MFA methods are assigned to individual users and shall not be shared, transferred, loaned, or used by any other individual under any circumstances.

7. MFA methods, including hardware tokens, software authenticators, or other approved mechanisms, are uniquely associated with an individual user account and must be protected from unauthorized use.

8. Upon termination of employment, contract, or authorized access, or when access is no longer required, ITS shall be notified immediately so identification cards and MFA methods can be deactivated. ITS retains authority to immediately revoke access without prior notice where necessary to protect County systems, facilities, or data.

9. Cards and tokens must be returned to the ITS Department. The Department Head of the department where the person was assigned is responsible for ensuring that the card is surrendered before the person leaves the County of Sullivan premises. It is the responsibility of the Department Head to return all surrendered cards and tokens to ITS for cataloging, deactivation or destruction, and in the case of tokens, recirculation/reissue.

10. Temporary cards may be issued by a department to eligible persons for a limited time period (e.g., when an individual provides volunteer or special services), and must be returned to the issuing department by the end of the authorized period. Each department will be responsible for logging in/out the temporary cards in their possession.

11. When County employees encounter individuals in secured non-public areas of County facilities or work sites, without appropriate identification and without authorized escorts, they should inquire whether the individual needs assistance. Any suspicious or unusual behavior should be immediately reported to management personnel. **NO ONE SHOULD CONFRONT THE INDIVIDUAL EXHIBITING SUSPICIOUS OR UNUSUAL BEHAVIOR FOR THE EMPLOYEE'S OWN SAFETY.**

12. The access system is set up to automatically suspend any card not used in over any 60-day period. The card will be suspended but the information will be retained in the system.

13. If a card or token does not work for any reason, please contact ITS via the help desk at x0110 or (845) 807-0110.

E. Authentication and Access Control

1. Multi-factor authentication (MFA) shall be required for access to County systems, applications, or services where determined by Information Technology Services based on risk, data sensitivity, or regulatory requirements.

2. Authentication requirements may vary based on system classification, user role, and risk level.

3. Authentication methods shall be configured, managed, and enforced by Information Technology Services and may include a combination of:
    - Something the user knows (e.g., password or passphrase);
    - Something the user has (e.g., token or device); and/or
    - Something the user is (e.g., biometric factor), where approved.

4. Users shall not attempt to bypass, disable, or interfere with authentication mechanisms or access controls.

5. Access granted through identification cards or MFA methods may be monitored, restricted, or revoked at any time in accordance with County policy.

F. Processing Requests for Identification Cards

1. Each employee is responsible for making a request, in person, to the ITS Department for a card. Initial requests for cards and photos are processed at the Sullivan County Government Center, 100 North Street, Monticello, NY 12701 in the ITS Department.

2. The ITS Department will supply the card with the carabiner, badge holder and/or lanyard.

G. Replacement of County Identification Cards and Tokens

1. A replacement card is required for a name change, transfer to a different department, change of job title, or for a lost, missing, stolen, or damaged card.

2. Employees/individuals must immediately notify their supervisor and Information Technology Services if their identification card or MFA method is lost, missing, stolen, damaged, or suspected to be compromised. Any suspected misuse or unauthorized access attempt must be reported in accordance with County incident reporting procedures.

3. An old or damaged card or token must be returned to the ITS Department before a replacement card is issued.

4. The ITS Department will assess employees/individuals a fee of $15.00 for each replacement card and $26.00 for each token replacement if their card/token was lost, missing or damaged. If the card/token is stolen and a police report is filed and produced, then there will be no charge. *(Note: All collective bargaining agreement provisions cover employees while they are on the job and working. Cards or tokens lost, missing or damaged outside of an employee's regular scheduled working hours or while off-premises (remote) are subject to this replacement fee. For purposes of this policy and as an example: even if working regularly scheduled hours but are remote, if your dog/puppy/child/significant other, etc., destroys your card/token at any time of day, this is not considered "unintentionally damaged" during work and you will be responsible for replacement fees.)*

5. New photographs and signatures (except for a name change) are not needed when replacing County identification cards since all original photographs are retained in the database.

6. Every five (5) years from the date of issue, the employee cards will be replaced free of charge and a new photograph will be taken. Employees will be responsible for contacting the ITS Department for an appointment.

7. MFA methods shall be maintained, replaced, or reissued based on operational, security, and lifecycle requirements as determined by Information Technology Services. This may include periodic replacement of hardware tokens or migration to updated authentication technologies.

H. Training and Enforcement

1. Each employee will be trained as to security needs of their work area as well as the building(s) in which they work.

2. It is the responsibility of Department Heads to ensure each employee has been trained and acknowledges the training they have received.

3. It is the responsibility of each County employee to comply with the requirements of this policy.

4. Failure to comply with identification, access control, or authentication requirements may result in suspension or revocation of access, disciplinary action, and/or other enforcement measures in accordance with County policy.

5. It is the responsibility of each County employee to report persons seen in restricted areas of a County facility who are not properly identified with an Employee ID card clearly displayed.

Title	Identification/Access Card and Multi-Factor Authentication (MFA) Policy			
Description	Establishing a process for issuing and controlling Identification/Access Cards to employees and certain visitors to County facilities in order to help maintain security.			
Created By	Lorne D. Green, CIO			
Date Created	August 27, 2018			
Maintained By	Lorne D. Green, CIO			
Version Number	**Modified By**	**Modifications Made**	**Date Modified**	**Status**
ITS2018-011.0	LDG	Initial creation edits after County Attorney and HR input.	08/31/2018	Final Draft
ITS2018-011.0	LDG	Added adoption date and resolution number to document header for publishing and distribution	09/25/2018	Adopted by the Legislature (Resolution #408-18)
ITS2018-011.1	LDG	Provisions for 2FA token replacement responsibility and fees added to policy	07/14/2023	Resubmit for Legislative approval in July 2023
ITS2018-011.1	LDG	Added adoption date and resolution number to document header and accept all amendments for publishing and distribution	07/20/2023	Adopted by the Legislature (Resolution #303-23)
SCITS-3030.003	LDG	2FA → Multi-Factor Authentication (MFA): The policy now reflects modern authentication methods, including hardware tokens, mobile authenticator applications, and other approved technologies. Integration with County Cybersecurity Framework: The policy is now aligned with the County's broader Information Technology and Cybersecurity Governance Policy (SCITS-0001.000), including Zero Trust principles and centralized authority under Information Technology Services (ITS). Strengthened Access Control Language: Clarifies that identification cards and authentication methods are part of a broader identity management system and are not standalone indicators of trust. Enhanced Enforcement Authority: Explicitly authorizes ITS to immediately revoke access to systems or facilities when necessary to protect County operations, systems, or data. Improved Incident Reporting Requirements: Requires immediate reporting of lost, stolen, or potentially compromised credentials and suspected misuse. Future-Proofing Authentication: Allows ITS to adapt authentication methods over time without requiring additional legislative updates.	04/06/2024	

Section 4 — Asset and Data Governance (4000 Series)

SCITS-4010.001 Policy – Data Storage

Title	Number
Data Storage	SCITS-4010.001
Creation Date: May 2026	
Modified Date:	

Purpose

The purpose of this policy is to establish requirements for the secure storage, handling, and protection of Sullivan County data across all systems, devices, and environments.

Sullivan County information is a critical public asset and must be stored only on systems that are authorized, managed, secured, and supported by the County. Proper control of data storage ensures that County information is protected against unauthorized access, loss, disclosure, alteration, or destruction, and that it remains available to support County operations, legal obligations, and public trust.

Unauthorized storage of County data significantly increases the risk of data breach, data loss, regulatory noncompliance, financial liability, and operational disruption.

Scope

This policy applies to:

- All Sullivan County departments, offices, agencies, and units;
- All employees, elected officials, contractors, consultants, vendors, interns, volunteers, and other authorized users; and
- All County data, regardless of format, classification, or storage medium.

This policy applies to all systems and devices used to access, process, transmit, or store County data, whether County-owned or personally owned.

General Policy

All County data shall be stored, processed, and accessed only on systems, platforms, and storage environments that are authorized and managed by Information Technology Services (ITS).

No user shall store, access, transmit, or maintain County data on any unauthorized system, device, or service.

Authorized Storage Locations

County data shall be stored only in:

- County-managed file storage systems and shared network drives;
- Approved enterprise systems and applications;
- County-approved cloud or Software-as-a-Service (SaaS) platforms that have been reviewed and authorized by ITS; and
- Other storage environments explicitly approved by the Commissioner of Information Technology / Chief Information Officer (CIO) or designee.

All County data must be stored in locations that are:

- Backed up in accordance with County policy;
- Protected by appropriate access controls;
- Monitored and secured by County systems; and
- Managed in accordance with retention, recovery, and legal requirements.

Prohibited Storage Practices

The following activities are strictly prohibited:

- Storing County data on local device storage (e.g., desktops, hard drives, or mobile devices) except where explicitly authorized and managed;
- Storing County data on removable media (e.g., USB drives, external hard drives, memory cards) unless approved and secured in accordance with County standards;
- Using personal devices or unmanaged systems to store or retain County data;
- Transmitting or storing County data through unauthorized systems, applications, or services; and
- Circumventing County storage controls, backup systems, or security protections.

Cloud Storage and External Services

Storage of County data in cloud-based or externally hosted services is permitted only where such services have been formally reviewed, approved, and managed by Information Technology Services.

Use of unauthorized cloud storage services, file-sharing platforms, or external storage providers is strictly prohibited.

Cloud-based storage that has not been approved by ITS shall not be used under any circumstances, regardless of cost, convenience, or funding source.

Data Access and Handling

County data shall be accessed and managed in a manner consistent with:

- Least privilege and business need;
- Applicable data classification and sensitivity;
- Legal, regulatory, and contractual requirements; and
- County policies governing acceptable use, security, and records management.

Users shall access data directly from authorized systems whenever feasible and shall not create unnecessary copies, downloads, or local storage of County data.

Ownership and Retention

All data created, received, stored, or transmitted in the course of County business is the property of Sullivan County.

- County data shall remain under County control regardless of where it is accessed;
- Data shall be retained, archived, or disposed of in accordance with applicable records retention requirements; and
- Upon separation from service, all County data remains the property of the County and shall not be removed, retained, or transferred without authorization.

Security and Protection

All authorized storage systems shall be subject to:

- Backup and recovery processes;
- Access control and authentication requirements;
- Monitoring, logging, and security controls; and
- Protection against unauthorized access, loss, or compromise.

Information Technology Services may implement technical controls to:

- Restrict unauthorized storage locations;
- Prevent data exfiltration;
- Enforce encryption or access requirements; and
- Detect and respond to policy violations.

Exceptions

Any exception to this policy must:

- Be formally requested in writing;

- Include a documented business justification and risk assessment; and
- Receive explicit written approval from the CIO or designee.

Approved exceptions may be subject to additional safeguards, limitations, or review.

Enforcement

All users are required to comply with this policy and to report any known or suspected violations to Information Technology Services or appropriate County leadership.

Failure to comply may result in:

- Removal or restriction of access to County systems;
- Removal or deletion of improperly stored data;
- Administrative or disciplinary action, up to and including termination; and/or
- Civil or criminal penalties where applicable.

Information Technology Services reserves the right to take immediate action to protect County systems and data, including restricting access, isolating systems, or removing unauthorized storage locations.

Disclaimer

Sullivan County assumes no responsibility for data stored outside of authorized systems or in violation of this policy. Unauthorized storage of County data may result in loss, exposure, or compromise of information, and such data may not be recoverable.

SCITS-4020.001 Policy – Data Backups

Title	Number
Data Backups	SCITS-4020.001
Creation Date: May 2026	
Modified Date:	

Departments, as information owners, are responsible for defining data retention, backup, and recovery requirements based on legal, regulatory, and operational needs.

Where such requirements are not defined, the County shall apply default retention and backup standards optimized for operational efficiency, storage management, and risk reduction.

Purpose

The purpose of this policy is to establish standards, procedures, and controls for the backup, retention, protection, and recovery of Sullivan County data stored on County-managed systems.

Sullivan County recognizes that reliable data backup and recovery capabilities are critical to ensuring business continuity, disaster recovery, cybersecurity resilience, and restoration of services following system failure, data corruption, or cyber incident.

This policy is intended to:

- Ensure the availability and recoverability of County data;
- Support disaster recovery and business continuity operations;
- Protect against data loss due to system failure, human error, or cybersecurity incidents;
- Establish consistent backup and retention standards; and
- Define roles and responsibilities for backup management and data protection.

Scope

This policy applies to:

- All County-owned, County-managed, or County-supported servers, storage systems, and infrastructure, including on-premises, cloud, and hybrid environments;
- All data stored within County-managed systems, including production, staging, and backup environments; and
- All systems and platforms under the administration of Information Technology Services.

This policy is primarily intended to support **system-level backup and disaster recovery operations**.

This policy does **not** apply to:

- Application-level backups managed within individual software systems (unless integrated into County backup strategy); or
- Data stored solely on unmanaged or unauthorized devices.

Data stored on individual desktops, laptops, or mobile devices is not included in system-level backup processes. Users are required to store all work-related data on County-managed systems or approved platforms to ensure proper backup and protection.

General Policy

The backup and recovery of County data shall be centrally managed by Information Technology Services.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, shall have authority over:

- Backup architecture, systems, and technologies;
- Backup frequency, retention, and recovery standards;
- Storage locations and security of backup data;
- Testing and validation of backup and recovery processes; and
- Enforcement of compliance with this policy.

All County systems and data within scope shall be included in a managed backup program unless explicitly exempted by Information Technology Services.

Backup Standards

Information Technology Services shall implement and maintain backup processes that ensure data can be restored within acceptable timeframes based on operational and business requirements.

At a minimum:

- **Full backups** shall be performed on a regularly scheduled basis;
- **Incremental or differential backups** shall be performed between full backups to capture changes; and
- Backup schedules shall be defined and maintained based on system criticality and operational needs.

Backup processes shall be:

- Automated wherever feasible;
- Monitored for successful completion; and
- Configured to alert on failures or anomalies.

Backup failures or anomalies shall be investigated, documented, and remediated in a timely manner in accordance with Information Technology Services procedures.

Retention Requirements

Backup data shall be retained in accordance with operational, legal, and regulatory requirements. This is not records retention. Backup retention periods defined in this policy are for disaster recovery purposes only and do not supersede or replace records retention requirements established by New York State Archives or applicable law.

At a minimum:

- Backup data shall be retained for a **minimum of thirty (30) days**;
- Standard retention shall not exceed **ninety (90) days**, unless otherwise required; and
- Extended retention may be applied where required for:
    - Legal hold;
    - Regulatory compliance (e.g., HIPAA, CJIS, Article 28);
    - Financial or audit requirements; or
    - Business or operational needs.

Retention schedules shall be defined and enforced by Information Technology Services. Where data is subject to legal hold, litigation, investigation, or audit, backup retention and deletion processes shall be suspended or modified as necessary to preserve relevant data in accordance with direction from the County Attorney.

Security of Backup Data

All backup data shall be protected to ensure confidentiality, integrity, and availability.

Security controls shall include, but are not limited to:

- Encryption of backup data at rest and in transit;
- Access controls restricting backup access to authorized personnel;
- Segregation of backup systems from production environments where feasible;
- Protection against unauthorized modification or deletion; and
- Monitoring and logging of backup access and activity.

Backup systems shall be protected against cybersecurity threats, including ransomware, through appropriate safeguards such as immutability, access restrictions, and network segmentation where feasible.

Backup Storage and Resilience

Backup data shall be stored in a manner that supports recovery from localized and widespread incidents.

Where feasible, backup strategies shall incorporate:

- Offsite or geographically separate storage;
- Cloud-based or secondary data center replication; and/or
- Isolated or immutable backup storage.

Storage methods shall be selected based on risk, system criticality, and operational requirements.

Recovery and Restoration

Information Technology Services shall maintain the capability to restore data and systems from backups in a timely and controlled manner.

Recovery processes shall:

- Be documented and tested periodically;
- Support restoration of systems, applications, and data; and
- Be prioritized based on system criticality and operational impact.

The CIO shall have authority to prioritize recovery efforts in alignment with:

- Business continuity requirements;
- Public safety and health services; and
- Operational priorities of the County.

System Recovery Prioritization

Sullivan County shall maintain a formal system recovery prioritization framework based on Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

This framework shall:

- Classify systems based on operational criticality, public safety impact, and regulatory requirements;
- Define recovery priorities and restoration sequencing during incidents; and
- Be maintained and updated by Information Technology Services.

Detailed system classifications, recovery tiers, and associated RTO/RPO values shall be documented in County-controlled standards or operational procedures.

Departments shall maintain documented recovery procedures for critical systems and data under their authority, coordinated with Information Technology Services.

Backup Testing and Validation

Backup and recovery processes shall be tested periodically to ensure reliability and effectiveness.

Testing shall include:

- Verification of backup integrity;
- Restoration testing of selected systems or data; and
- Validation of recovery procedures and timelines.

Backup and recovery processes shall be tested periodically to validate effectiveness and ensure the ability to restore systems and data within acceptable timeframes. Testing frequency shall be determined by Information Technology Services based on system criticality and risk.

User Responsibilities

All users are responsible for:

- Storing work-related data on County-managed systems or approved platforms;
- Ensuring critical data is not stored solely on local or unmanaged devices; and
- Saving and closing files appropriately to ensure data is captured in scheduled backups.

Files left open or unsaved during backup processes may not be captured.

Failure to store data in approved locations may result in permanent data loss for which the County assumes no responsibility.

Prohibited Activities

The following activities are strictly prohibited:

- Storing County data exclusively on local or unmanaged devices;
- Circumventing or interfering with backup processes or systems;
- Unauthorized access to backup systems or data; and
- Deleting or altering backup data outside of approved processes.

Incident Response Integration

Backup systems and data shall be integrated into the County’s Incident Response and Business Continuity framework.

In the event of a cybersecurity incident:

- Backup data may be used to restore affected systems;
- Access to backup systems may be restricted to prevent compromise; and
- Recovery actions shall be coordinated under the authority of the CIO.

Where necessary, restoration from backups may take precedence over full forensic preservation in accordance with the County's Incident Response Policy.

Enforcement

Failure to comply with this policy may result in:

- Revocation of system access;
- Disciplinary action;
- Termination of employment or contract; and/or
- Legal or regulatory action.

Disclaimer

Sullivan County assumes no liability for loss of data that is not stored on County-managed or approved systems, or that is otherwise outside the scope of this policy.

SCITS-4030.001 Policy – Email Retention and Archiving

Title	Number
Email Retention and Archiving	SCITS-4030.001
Creation Date: May 2026	
Modified Date:	

Purpose

Sullivan County is committed to maintaining email records in accordance with applicable laws, regulations, and sound records management practices.

Email messages created, received, or maintained by Sullivan County may constitute official County records and are subject to the New York State Freedom of Information Law (FOIL), Local Government Records Law, and other applicable legal and regulatory requirements.

The purpose of this policy is to establish standards for the retention, archiving, retrieval, and disposition of email records to ensure legal compliance, operational integrity, and the preservation of public records.

Scope

This policy applies to:

- All Sullivan County email systems and services, whether hosted on-premises or in the cloud;
- All email messages sent or received using a County-issued email account; and
- All employees, elected officials, contractors, consultants, and other individuals using County email systems.

This policy applies regardless of the device used to access email.

Definition of a Business Record

An email message is considered a **business record** if it is created, received, or maintained in the ordinary course of County business and has administrative, legal, fiscal, or operational value.

Examples of business records include, but are not limited to:

- Official communications, directives, or decisions;

- Contracts, agreements, or negotiations where terms are established;
- Policy statements or formal guidance; and
- Any communication that serves as the official record of County business activity.

Emails that are transitory in nature—such as drafts, informal communications, duplicates, or personal messages—may not constitute business records unless they are the only record of a business activity.

The determination of whether an email constitutes a business record is the responsibility of the originating or receiving department, in accordance with applicable records retention schedules.

General Policy

Email is governed both as a communication tool and as an official record. All inbound and outbound email messages transmitted through County systems shall be automatically captured and archived by County-approved systems managed by Information Technology Services.

Archived email shall be:

- Retained in a secure, tamper-resistant environment;
- Indexed and searchable, including metadata, message content, and attachments; and
- Maintained in accordance with applicable retention schedules and legal requirements.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, is responsible for the administration, security, and operation of email archiving systems. Determination of record retention requirements remains the responsibility of departments in accordance with applicable laws and records management guidance.

Retention periods for email records shall comply with:

- New York State Local Government Records Retention Schedules;
- FOIL requirements;
- Any applicable federal or state regulatory requirements; and
- County-specific records management policies.

Where retention requirements exceed system-based archiving durations, departments are responsible for ensuring appropriate preservation of such records in approved systems or formats.

Litigation Hold and Legal Preservation

In the event of actual or reasonably anticipated litigation, investigation, audit, or legal action, Sullivan County is required to preserve all relevant records, including email.

Upon notification by the County Attorney or Corporate Compliance Office, a **litigation hold** shall be implemented. This directive:

- Suspends normal retention and disposition practices;
- Requires preservation of all relevant email and related records; and
- Applies to all affected individuals and departments.

Failure to comply with a litigation hold may result in legal consequences for both the individual and the County.

Prohibition on Unauthorized Deletion

It is a violation of this policy to intentionally delete, destroy, or alter email records that are subject to retention requirements, legal hold, or regulatory obligation.

Users must not take any action to circumvent, disable, or interfere with County email archiving systems.

If an email believed to be a business record is accidentally deleted, the user must immediately notify Information Technology Services, as recovery may be possible.

Any suspected or known unauthorized destruction of email records must be reported to a Department Head, Information Technology Services, or the appropriate oversight authority.

Monitoring and Access

Archived email records may be accessed, retrieved, and reviewed:

- In response to FOIL requests;
- For legal, audit, or compliance purposes;
- For operational continuity or investigation; or
- As otherwise authorized by law or County policy.

Access to archived email is controlled and logged, and shall be conducted in accordance with applicable laws, policies, and due process.

Users should have no expectation of privacy in email communications conducted on County systems.

Enforcement

Failure to comply with this policy may result in:

- Disciplinary action, up to and including termination;
- Legal action, where applicable; and/or
- Personal liability under applicable laws and regulations.

Disclaimer

Sullivan County retains ownership of all email communications transmitted through its systems. Email records are subject to disclosure in accordance with applicable laws and regulations.

SCITS-4050.001 Policy – Information Technology Asset Disposal and Destruction

Title	Number
Information Technology Asset Disposal	SCITS-4050.001
Creation Date: May 2026	
Modified Date:	

Purpose

The purpose of this policy is to establish standards, procedures, and controls for the secure, lawful, and environmentally responsible disposal of Sullivan County-owned information technology (IT) assets.

All surplus, obsolete, or retired IT assets—including computers, servers, mobile devices, and networking equipment—must be disposed of in a manner that protects County data, complies with applicable laws and regulations, and ensures responsible stewardship of public resources.

Scope

This policy applies to:

- All non-leased IT assets owned by Sullivan County, including but not limited to desktops, laptops, servers, printers, mobile devices, storage media, and network equipment;
- All County departments and personnel involved in the management, use, or disposition of such assets; and
- All stages of the asset lifecycle once equipment is designated for retirement, reassignment, or disposal.

Leased or vendor-owned equipment shall be returned or disposed of in accordance with contractual terms, with oversight by Information Technology Services.

Definitions

- **IT Asset**: Any hardware or associated media used to store, process, or transmit County data.
- **Disposal**: The final disposition of IT assets through resale, reassignment, recycling, donation, or destruction.

- **Obsolete**: Equipment that no longer meets operational, security, or support requirements as determined by Information Technology Services.
- **Surplus**: Equipment that is no longer required for its original purpose but remains functional.
- **Beyond Reasonable Repair**: Equipment for which repair is not cost-effective relative to replacement.
- **Data Sanitization**: The process of permanently removing or destroying data from storage media to prevent recovery.

General Policy

All IT asset disposal activities shall be centrally managed and controlled by Information Technology Services.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has sole authority over:

- Classification of IT assets as surplus, obsolete, or beyond reasonable repair;
- Approval of disposal methods and processes;
- Selection and oversight of third-party disposal or recycling vendors; and
- Verification that all data has been securely sanitized prior to disposal.

All IT assets must be tracked through an official County asset inventory system, and their disposition status must be documented prior to and following disposal.

The disposal, sale, transfer, or donation of any County-owned IT asset shall require approval in accordance with County procurement policies and, where applicable, formal authorization by the County Legislature.

Acceptable Methods of Disposal

IT assets may be disposed of through one or more of the following approved methods:

- Reassignment for continued use in a less critical function;
- Trade-in or exchange as part of procurement of replacement equipment;
- Resale or auction through approved channels;
- Donation in accordance with County policies and legal requirements;
- Recycling through certified and approved e-waste vendors; or
- Physical destruction and disposal through licensed service providers.

All disposal methods must comply with applicable local, state, and federal laws and regulations.

Data Sanitization and Decommissioning

All IT assets containing County data must be securely sanitized prior to disposal.

Information Technology Services shall ensure that:

- All data is permanently removed using approved data sanitization methods consistent with industry standards (e.g., NIST-compliant methods);
- Storage media is overwritten, degaussed, or physically destroyed as appropriate based on risk and device type; and
- All County-owned software, configurations, and access controls are removed.

No IT asset may be disposed of, transferred, or reassigned until data sanitization has been verified and documented.

Media Destruction Requirements

All storage media containing County data shall be subject to risk-based destruction requirements as determined by Information Technology Services.

Destruction Triggers
Physical destruction of storage media shall be required where:

- The media contains regulated or sensitive data, including but not limited to PII, PHI, CJI, or financial information;
- Data sanitization cannot be reliably verified;
- The asset is damaged, inoperable, or otherwise unsuitable for secure reuse;
- Required by legal, regulatory, or contractual obligations.

Approved Destruction Methods
Approved destruction methods shall include:

- Mechanical shredding;
- Crushing or pulverization;
- Degaussing (where applicable); and/or
- Other methods approved by Information Technology Services consistent with recognized standards (e.g., NIST SP 800-88).

Destruction Execution Requirements
All destruction activities shall:

- Be performed by authorized Information Technology Services personnel or approved, certified vendors;
- Be documented, including asset identification, method of destruction, date, and responsible party;
- Be witnessed by authorized personnel where required based on data sensitivity or risk; and
- Ensure that data is rendered irrecoverable.

Where destruction is performed by a third party, a Certificate of Destruction shall be obtained and retained.

Prohibited Practices
Under no circumstances shall storage media containing County data be discarded intact in general waste or recycling streams.

Media Chain-of-Custody and Tracking

All IT assets and storage media designated for disposal, sanitization, or destruction shall be subject to formal chain-of-custody controls to ensure accountability, traceability, and protection against unauthorized access or loss.

Information Technology Services shall maintain documented custody records for all such assets from the point of decommissioning through final disposition.

Chain-of-custody documentation shall include, at minimum:

- Asset identification (e.g., asset tag, serial number, device type);
- Assigned owner or originating department;
- Date and method of decommissioning;
- Data classification level (where applicable);
- Sanitization method performed (if applicable);
- Transfer history, including individuals or entities assuming custody;
- Dates and times of custody transfers;
- Final disposition method (e.g., resale, recycling, destruction); and
- Verification of completion, including Certificates of Destruction where applicable.

At all times, IT assets awaiting disposal shall be stored in secure, access-controlled locations with restricted access limited to authorized personnel.

When custody of assets is transferred to a third-party vendor:

- Transfer shall be formally documented and acknowledged;
- The vendor shall assume responsibility under contractual security and confidentiality requirements; and
- The County shall retain the right to audit custody and destruction records.

Any break in chain-of-custody, loss of asset, or discrepancy in records shall be treated as a potential security incident and handled in accordance with the County's Incident Response Policy.

Physical Asset Handling

Prior to disposal:

- All County identification tags, asset labels, and markings must be removed;
- Equipment must be inspected to ensure no residual data or identifying information remains; and
- Any reusable components may be retained for operational use where appropriate.

Equipment deemed beyond reasonable repair may be dismantled for usable parts at the discretion of Information Technology Services.

Environmental and Regulatory Compliance

All disposal activities must comply with applicable environmental laws and regulations governing electronic waste and hazardous materials.

Where required, disposal vendors must be certified and capable of properly handling and documenting the removal and processing of hazardous components.

Information Technology Services shall ensure that appropriate documentation is obtained from vendors to verify compliant disposal practices.

Third-Party Vendors

All third-party vendors involved in asset disposal must be:

- Approved by Information Technology Services;
- Contractually obligated to comply with County security, confidentiality, and disposal requirements; and
- Required to provide documentation verifying data destruction and proper disposal.

The County reserves the right to audit vendor practices and require proof of compliance.

Financial Accountability

Where disposal results in revenue (e.g., resale or auction):

- All proceeds must be properly documented and remitted to the County Treasurer; and
- Disposal activities must be coordinated with Purchasing, Finance, and other appropriate County offices.

Efforts should be made, where feasible, to maximize the residual value of IT assets in a manner consistent with security and operational requirements.

Prohibited Activities

The following are strictly prohibited:

- Disposal of IT assets without approval from Information Technology Services;
- Disposal of equipment without verified data sanitization;
- Unauthorized sale, transfer, or personal use of County-owned IT assets; and
- Circumventing established disposal procedures or controls.

Enforcement

Failure to comply with this policy may result in:

- Disciplinary action, up to and including termination;
- Financial liability for damages or loss; and/or
- Legal action where applicable.

Disclaimer

Sullivan County assumes no liability for damages resulting from unauthorized or improper disposal of IT assets in violation of this policy.

SCITS-4060.001 Policy – Removable Media and Portable Storage Policy

Title	Number
Removable Media and Portable Storage Policy	**SCITS-4060.001**

Creation Date: **May 2026**

Modified Date:

Purpose

Removable media and portable storage devices present significant cybersecurity and data protection risks due to their portability, ability to store large volumes of data, and potential to introduce malware or enable unauthorized data transfer.

The purpose of this policy is to establish standards, procedures, and restrictions governing the use of removable media to protect Sullivan County systems, networks, and data from unauthorized access, data loss, malware infection, and other security threats.

Scope

This policy applies to:

- All Sullivan County employees, elected officials, contractors, consultants, vendors, interns, and other authorized users;
- All County-owned and personally owned removable media devices;
- All County systems, networks, and technology resources; and
- All data stored on or transferred using removable media.

This policy applies regardless of ownership of the device and includes any hardware or software capable of storing or transferring County data outside of controlled systems.

Removable media includes, but is not limited to:

- USB flash drives and external storage devices;
- Memory cards (e.g., SD, microSD, CompactFlash);
- External hard drives and solid-state drives;
- Mobile devices capable of storage (e.g., smartphones, tablets);

- Digital cameras and media devices with storage capability;
- Optical media (e.g., CDs, DVDs);
- Any device capable of transferring data via wired or wireless means, including Bluetooth or similar technologies.

General Policy

The use of removable media for County business is restricted and permitted only where a legitimate business need exists and where such use has been approved by Information Technology Services.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has authority to approve, restrict, or prohibit the use of removable media and to implement technical controls to enforce this policy.

Only removable media devices issued, approved, or managed by Information Technology Services may be used to store or transfer County data.

Unauthorized removable media devices are prohibited from being connected to County systems or networks.

Authorized Use

Where approved, removable media may be used for legitimate County business purposes in accordance with this policy and all applicable data protection requirements.

All removable media devices used for County purposes must:

- Be issued or explicitly approved by Information Technology Services;
- Utilize encryption where technically feasible;
- Be used only for authorized business purposes; and
- Be handled in a manner that protects County data from unauthorized access, loss, or disclosure.

Users must maintain physical control of removable media devices at all times and take reasonable precautions to prevent loss, theft, or misuse.

Data Storage Requirements

Removable media shall not be used as a primary or permanent storage location for County data.

All County data must be stored on approved County-managed systems, including designated network storage locations or other systems approved by Information Technology Services.

Temporary use of removable media for data transfer may be permitted where necessary; however, data must be transferred to approved storage locations as soon as practicable and removed from the removable device.

Storage of confidential, sensitive, or regulated data on removable media is prohibited unless explicitly authorized and appropriately secured in accordance with County standards.

Security Controls

Information Technology Services shall implement technical and administrative controls to manage the use of removable media, which may include:

- Restricting or disabling USB and other external ports;
- Allowing access only to approved devices;
- Automatically scanning removable media for malware upon connection;
- Monitoring and logging data transfer activity; and
- Enforcing encryption and other data protection measures.

Users shall not attempt to bypass or disable these controls.

Connection of removable media may result in performance impacts due to required security scanning.

Prohibited Activities

The following activities are strictly prohibited:

- Connecting unauthorized removable media to County systems or networks;
- Storing County data on personal or unapproved devices;
- Using removable media to bypass security controls or monitoring;
- Transferring County data to unauthorized systems or locations;
- Storing passwords, credentials, or other sensitive authentication information on removable media;
- Using removable media in a manner that introduces security risk or violates County policy; and
- Any activity that results in unauthorized disclosure, alteration, or destruction of County data.

User Responsibilities

Users of removable media are responsible for:

- Ensuring that devices are used only for authorized purposes;
- Protecting devices from loss, theft, or unauthorized access;
- Ensuring that any system used in conjunction with removable media meets County security requirements;
- Promptly reporting any loss, theft, or suspected compromise of removable media; and

- Complying with all County policies and applicable laws.

Incident Reporting

Any loss, theft, misuse, or suspected compromise of removable media or data must be reported immediately to a supervisor, Department Head, Information Technology Services, or the Chief Information Officer (CIO).

Monitoring and Enforcement

Sullivan County reserves the right, subject to applicable law, to monitor, restrict, and audit the use of removable media to ensure compliance with this policy.

Violations of this policy may result in:

- Immediate restriction or revocation of access;
- Removal of unauthorized devices or data;
- Disciplinary action, up to and including termination; and/or
- Legal action where applicable.

Disclaimer

Sullivan County assumes no liability for damages arising from unauthorized or improper use of removable media, except as otherwise required by law.

Section 5 — Network and Infrastructure Security (5000 Series)

SCITS-5000.001 Policy – Network Access and Secure Connectivity Policy

Title	Number
Network Access and Secure Connectivity Policy	**SCITS-5000.001**
Creation Date: **May 2026**	
Modified Date:	

Purpose

Access to Sullivan County networks, systems, and applications is essential to conducting County business; however, such access introduces significant cybersecurity, operational, and legal risks if not properly controlled.

The purpose of this policy is to establish standards, procedures, and restrictions governing access to County networks and applications to ensure that all access is secure, authorized, and consistent with the protection of County systems, data, and services.

All access to County resources must utilize County-approved methods and controls designed to prevent unauthorized use, malicious activity, data loss, and system compromise.

Scope

This policy applies to:

- All Sullivan County employees, elected officials, contractors, consultants, vendors, interns, and other authorized users;
- All devices used to access County systems, whether County-owned or personally owned;
- All methods of access, including on-site, remote, wireless, and virtual connections; and
- All County systems, networks, applications, and data resources.

Access to County systems is a privilege, not a right, and shall be granted only where a valid business need exists and appropriate authorization has been obtained.

General Policy

All access to Sullivan County networks and applications shall be centrally managed and controlled by Information Technology Services.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has authority over all network access methods, authentication requirements, security controls, and connection standards.

Users shall access County systems only through approved and secured methods, which may include managed network connections, virtual private network (VPN) access, virtual desktop infrastructure (VDI), or other secure access technologies designated by Information Technology Services.

Departments are prohibited from establishing independent or unauthorized networks, systems, or access methods that connect to or interact with County resources.

Access Control and Authentication

All access to County systems shall require:

- Unique user identification;
- Strong authentication in accordance with County policy;
- Multi-factor authentication (MFA) where required; and
- Authorization based on job role and business need.

Authentication and access controls shall be enforced through centrally managed systems and may include encryption, conditional access, device compliance checks, and other security measures.

Users are responsible for protecting their credentials and must not share or disclose access information.

Secure Use Requirements

Users accessing County systems must:

- Use only approved devices, systems, and connection methods;
- Ensure that devices meet County security requirements, including endpoint protection and patching;
- Follow all applicable County policies, including acceptable use, password, and data protection policies;
- Maintain secure connections and avoid use of unsecured or untrusted networks where possible; and
- Conduct County business in a manner that is appropriate, lawful, and consistent with County standards.

Use of personal email accounts or unauthorized communication platforms to conduct County business is prohibited.

Prohibited Activities

The following activities are strictly prohibited:

- Accessing County systems through unauthorized networks or methods;
- Connecting devices that do not meet County security requirements;
- Modifying, bypassing, or attempting to circumvent security controls;
- Establishing unauthorized network connections (e.g., dual-homing, rogue wireless access points);
- Using County network access for unlawful, inappropriate, or non-business purposes; and
- Any activity that exposes County systems or data to unnecessary risk.

Monitoring and Session Management

All network access and activity may be monitored, logged, and analyzed by Sullivan County to ensure security, detect unauthorized activity, and support operational and compliance requirements.

Session controls, including timeouts, re-authentication requirements, and connection limits, shall be defined and enforced by Information Technology Services based on current security standards and operational needs.

Users acknowledge that there is no expectation of privacy when accessing County systems.

Incident Reporting

Users must immediately report any of the following:

- Suspected unauthorized access;
- Lost or compromised devices used for access;
- Suspicious activity or system behavior; or
- Any potential security incident involving County systems.

Reports shall be made to a supervisor, Department Head, Information Technology Services, or in accordance with the County's Security Incident and Data Breach Reporting Policy.

Device and Connectivity Responsibility

Users are responsible for ensuring that devices used to access County systems are:

- Securely configured;
- Protected against malware and unauthorized access; and

- Not simultaneously connected to unsecured or conflicting networks in a manner that introduces risk.

Any damage, loss, or compromise of devices used for access must be reported immediately.

Enforcement

Failure to comply with this policy may result in:

- Suspension or revocation of network access;
- Restriction of system privileges;
- Disciplinary action, up to and including termination; and/or
- Legal action where applicable.

Disclaimer

Sullivan County assumes no liability for damages resulting from unauthorized or improper use of network access in violation of this policy, except as otherwise required by law.

SCITS-5010.001 Policy – Remote Access and External Connectivity

Title	Number
Remote Access and External Connectivity	**SCITS-5010.001**

Creation Date: **May 2026**

Modified Date:

Purpose

Remote access to Sullivan County systems enables continuity of operations and workforce flexibility; however, it introduces elevated cybersecurity risks due to connections originating outside of County-controlled environments.

The purpose of this policy is to establish standards, procedures, and restrictions governing remote access to Sullivan County networks, systems, and applications in order to ensure that such access is secure, authorized, and properly controlled.

All remote access must utilize County-approved methods and security controls designed to protect County systems, data, and services from unauthorized access, compromise, or misuse.

Scope

This policy applies to:

- All Sullivan County employees, elected officials, contractors, consultants, vendors, interns, and other authorized users;
- All devices used to access County systems remotely, whether County-owned or personally owned;
- All forms of remote connectivity, including home networks, public networks, wireless hotspots, mobile networks, and third-party Internet service providers; and
- All County systems, applications, and data accessed from outside County-controlled facilities.

Remote access is defined as any connection to County systems from an external location, including but not limited to residences, hotels, public spaces, mobile devices, or satellite offices.

Remote access privileges are granted based on business need and require approval by the user's Department Head and Information Technology Services.

General Policy

All remote access to Sullivan County systems shall be centrally managed and controlled by Information Technology Services.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has sole authority over:

- Remote access methods and technologies;
- Authentication and security requirements;
- Device compliance standards; and
- Approval, restriction, or revocation of remote access privileges.

Only County-approved remote access solutions may be used. These may include secure virtual private network (VPN) access, virtual desktop infrastructure (VDI), or other technologies designated by Information Technology Services.

Unauthorized remote access methods, tools, or configurations are strictly prohibited.

Authentication and Security Requirements

All remote access must meet the following minimum security requirements:

- Multi-factor authentication (MFA) using County-approved methods (e.g., DUO token, DUO Mobile application, phone call, or text message);
- Strong authentication credentials in accordance with County Password Policy;
- Encrypted communication channels;
- Device compliance with County security standards; and
- Continuous monitoring and logging of access activity.

Access may be restricted or blocked based on risk, device posture, location, or other security conditions as determined by Information Technology Services.

Device and Endpoint Requirements

Devices used for remote access must:

- Meet County security configuration standards;
- Have current endpoint protection and security controls installed;
- Be maintained with current updates and patches; and
- Be protected against unauthorized access through physical and logical safeguards.

Information Technology Services reserves the right to deny or terminate access from any device that does not meet these requirements.

Use of Public or Untrusted Networks

Users may access County systems from public or third-party networks (e.g., wireless hotspots) only through County-approved secure access methods.

Users must exercise caution when using public networks and avoid accessing sensitive information where risk cannot be reasonably mitigated.

Under no circumstances may users bypass County security controls when connecting from public or untrusted networks.

User Responsibilities

Users with remote access privileges must:

- Use only County-approved access methods and technologies;
- Protect authentication credentials and MFA devices;
- Ensure devices are secured when not in use;
- Avoid conducting County business on unsecured or shared devices;
- Immediately disconnect from County systems when access is no longer required; and
- Comply with all applicable County policies, including acceptable use, data protection, and cybersecurity policies.

Use of personal email accounts or unauthorized platforms to conduct County business is strictly prohibited.

Prohibited Activities

The following activities are strictly prohibited:

- Use of unauthorized remote access tools or services;
- Circumventing or attempting to bypass County security controls;
- Connecting to County systems using devices that do not meet security requirements;
- Simultaneous connection to insecure or conflicting networks in a manner that increases risk;
- Sharing access credentials or MFA methods; and
- Any use of remote access for unlawful, inappropriate, or non-business purposes.

Monitoring and Logging

All remote access sessions may be monitored, recorded, and analyzed to:

- Detect unauthorized access or suspicious activity;
- Ensure compliance with County policies; and
- Support incident response and legal or regulatory requirements.

Users acknowledge that there is no expectation of privacy when accessing County systems remotely.

Incident Reporting

Users must immediately report:

- Lost, stolen, or compromised devices used for remote access;
- Suspected unauthorized access or credential compromise;
- Suspicious activity or system anomalies; and
- Any potential security incident involving remote access.

Reports shall be made to a supervisor, Department Head, Information Technology Services, or in accordance with the County's Security Incident and Data Breach Reporting Policy.

Access Suspension and Revocation

Remote access privileges may be suspended or revoked at any time by Information Technology Services for:

- Security concerns;
- Policy violations;
- Changes in job responsibilities; or
- Operational or risk management reasons.

Accounts that remain inactive for a period defined by Information Technology Services may be disabled or removed.

Enforcement

Failure to comply with this policy may result in:

- Immediate suspension or revocation of remote access;
- Disciplinary action, up to and including termination; and/or
- Legal action where applicable.

Disclaimer

Sullivan County assumes no liability for damages arising from unauthorized or improper use of remote access in violation of this policy, except as otherwise required by law.

SCITS-5020.001 Policy – County Wireless Network Access

Title	Number
County Wireless Network Access	SCITS-5020.001
Creation Date: May 2026	
Modified Date:	

Purpose

Sullivan County provides wireless networking capabilities to support authorized business operations; however, wireless access introduces increased cybersecurity risk due to its broadcast nature and potential exposure to unauthorized users and devices.

The purpose of this policy is to establish standards, procedures, and restrictions governing the use of County-provided wireless networks to ensure that all wireless access is secure, authorized, and properly controlled.

This policy is intended to protect Sullivan County technology resources—including data, systems, networks, and applications—from unauthorized access, compromise, or misuse.

Scope

This policy applies to:

- All Sullivan County employees, elected officials, contractors, consultants, vendors, interns, and other authorized users;
- All devices connecting to County wireless networks, whether County-owned or personally owned; and
- All wireless infrastructure, including access points, controllers, and related networking components.

Access to County wireless networks is a privilege, not a right, and is granted only where a valid business need exists and appropriate authorization has been obtained.

General Policy

All County wireless networks, infrastructure, and access controls shall be centrally managed and controlled by Information Technology Services.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has sole authority over:

- Wireless network design, deployment, and configuration;
- Access control and authentication requirements;
- Device eligibility and network segmentation;
- Security standards and monitoring; and
- Approval or denial of wireless access requests.

Only County-approved wireless networks and access points may be used to access County systems and resources.

Authorized Devices and Access

Only devices that meet County security requirements and are approved by Information Technology Services may connect to County wireless networks.

Information Technology Services may permit limited access for non-County devices (e.g., guest devices, vendor equipment, or public access scenarios) where appropriate. Such access shall be:

- Explicitly authorized;
- Segmented from internal County systems where required; and
- Subject to appropriate security controls and monitoring.

All requests for wireless access must be submitted through appropriate channels and approved by Information Technology Services.

County Internal Wireless Network Configuration

County-operated internal wireless networks used for access to Sullivan County systems may be configured as non-broadcast (hidden SSID) networks and are restricted to authorized, managed County devices only.

Connection to such networks shall require County-approved authentication, encryption, and device compliance controls. The use of a non-broadcast SSID is an operational measure to limit visibility and does not replace required security controls.

Security Requirements

All wireless access must comply with County cybersecurity policies and shall include, at a minimum:

- Strong authentication and access control mechanisms;
- Multi-factor authentication (MFA) where applicable;
- Encrypted communication protocols;

- Device compliance with County security standards; and
- Continuous monitoring and logging of network activity.

Users are responsible for safeguarding their credentials and must not share authentication information.

Network Segmentation and Isolation — Sullivan County wireless and network infrastructure shall be segmented to enforce strict separation between internal County systems and any guest, public, or non-County device access. Guest or external wireless networks shall be logically and technically isolated from internal County networks and shall not permit access to County systems, applications, or data. Information Technology Services shall implement and maintain appropriate controls—including network segmentation, firewalls, access control lists, and monitoring—to ensure that only authorized, authenticated, and compliant devices may access internal resources. Under no circumstances shall guest or unmanaged device traffic traverse or interact with internal County networks.

Acceptable Use

Use of County wireless networks must:

- Be limited to authorized County business purposes;
- Comply with all applicable County policies, including acceptable use, data protection, and cybersecurity policies; and
- Not interfere with network performance, security, or availability.

Limited guest or public access, where provided, shall be governed by restrictions defined by Information Technology Services.

Prohibited Activities

The following activities are strictly prohibited:

- Connecting unauthorized devices to County wireless networks;
- Attempting to bypass or circumvent wireless security controls;
- Installing or operating unauthorized wireless access points, routers, hotspots, or similar devices;
- Using wireless access for unlawful, inappropriate, or non-business purposes; and
- Any activity that introduces risk to County systems, data, or network integrity.

Monitoring and Enforcement

All wireless network activity may be monitored, logged, and analyzed to:

- Detect unauthorized access or suspicious activity;
- Ensure compliance with County policies; and
- Support incident response, audits, and legal or regulatory requirements.

Users acknowledge that there is no expectation of privacy when using County wireless networks.

Violations of this policy may result in:

- Immediate disconnection from the wireless network;
- Revocation of access privileges;
- Disciplinary action, up to and including termination; and/or
- Legal action where applicable.

Prohibition on Unauthorized Wireless Networks

Under no circumstances shall any County department, employee, contractor, or other individual install, operate, or maintain any wireless network, wireless access point, router, hotspot, or similar device that connects to or interacts with Sullivan County systems or infrastructure without the explicit written authorization of Information Technology Services.

Unauthorized wireless networks are strictly prohibited and may be disabled or removed immediately without notice.

Incident Reporting

Any suspected unauthorized wireless activity, device, or access must be reported immediately to Information Technology Services or in accordance with the County's Security Incident and Data Breach Reporting Policy.

Disclaimer

Sullivan County assumes no liability for damages arising from unauthorized or improper use of wireless networks in violation of this policy, except as otherwise required by law.

SCITS-5030.001 Policy – Endpoint Protection and Malware Defense Policy

Title	Number
Endpoint Protection and Malware Defense Policy	**SCITS-5030.001**

Creation Date: **May 2026**

Modified Date:

Purpose

Malware—including ransomware, viruses, worms, trojans, spyware, and other malicious code—poses a significant threat to Sullivan County's systems, data, and operations. Such threats may be introduced through email attachments, Internet downloads, compromised websites, removable media, or unauthorized applications and services.

A successful malware or ransomware incident can result in data loss, system disruption, financial impact, legal exposure, and damage to public trust.

The purpose of this policy is to establish requirements for the prevention, detection, response, and management of malware threats to protect Sullivan County's technology environment.

Scope

This policy applies to:

- All Sullivan County information systems, networks, and devices;
- All County-owned and personally owned devices used to access County systems;
- All users, including employees, elected officials, contractors, consultants, vendors, interns, and other authorized individuals; and
- All methods of access, including wired, wireless, remote access, and virtual private network (VPN) connections.

Devices include, but are not limited to, desktops, laptops, servers, mobile devices, and any system capable of connecting to County resources.

General Policy

Sullivan County shall maintain a centrally managed endpoint protection program designed to prevent, detect, and respond to malware and ransomware threats.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has authority over all endpoint security controls, including selection, configuration, deployment, monitoring, and enforcement of anti-malware and endpoint protection solutions.

All devices connecting to County systems or networks must have County-approved endpoint protection controls in place, including anti-malware and, where applicable, advanced endpoint detection and response (EDR/XDR) capabilities.

Information Technology Services shall determine and maintain approved security tools, configurations, and protection standards based on current threat conditions and best practices.

Endpoint Protection Requirements

All applicable systems must:

- Have County-approved endpoint protection software installed and actively running;
- Receive automatic updates to malware definitions, detection engines, and security configurations;
- Be configured to perform regular scans and real-time threat monitoring;
- Be centrally managed and monitored by Information Technology Services; and
- Not be altered, disabled, or bypassed by users.

Personally owned devices authorized to access County systems must meet equivalent security requirements as determined by Information Technology Services.

Devices that do not meet these requirements may be denied access to County systems.

Prohibited Activities

The following activities are strictly prohibited:

- Creating, introducing, or distributing malware, ransomware, or other malicious code;
- Downloading or installing unauthorized software that may introduce security risk;
- Disabling, modifying, or interfering with endpoint protection controls;
- Attempting to bypass security controls or monitoring systems; and
- Using County systems in any manner that introduces malware risk.

User Responsibilities

All users are responsible for exercising reasonable care to prevent malware infection, including:

- Avoiding opening suspicious email attachments or links;
- Downloading files only from trusted and authorized sources;
- Using only approved applications and services;
- Not connecting unauthorized devices or media to County systems; and
- Promptly reporting suspicious activity or potential threats.

Users shall comply with all County security policies and guidance issued by Information Technology Services.

Incident Response and Reporting

Any suspected or confirmed malware or ransomware incident must be reported immediately to Information Technology Services.

Users must not attempt to investigate, remove, or remediate malware without direction from Information Technology Services.

Upon detection or suspicion of infection:

- The affected device may be isolated or removed from the network;
- Access to systems may be restricted;
- Forensic or remediation actions may be initiated; and
- Recovery efforts will be managed by Information Technology Services.

Users shall cooperate fully with incident response efforts.

Device Isolation and Remediation

Any device suspected of being infected or compromised may be:

- Immediately disconnected or isolated from the network;
- Restricted from accessing County systems;
- Subject to analysis, remediation, or reimaging; and
- Returned to service only after being verified as secure by Information Technology Services.

Department Responsibilities

Departments are responsible for ensuring that all systems under their control comply with this policy and that users are aware of and adhere to required security practices.

Departments permitting the use of non-County devices for business purposes must ensure that such use complies with County security standards and is approved by Information Technology Services.

Monitoring and Enforcement

Sullivan County reserves the right, subject to applicable law, to monitor systems, devices, and network activity to detect and respond to malware threats.

Violations of this policy may result in:

- Immediate restriction or revocation of system access;
- Disciplinary action, up to and including termination; and/or
- Legal action where applicable.

Disclaimer

Sullivan County assumes no liability for damages resulting from malware or ransomware incidents where such incidents arise from failure to comply with this policy, except as otherwise required by law.

Section 6 — Acceptable Use and User Responsibilities (6000 Series)

The following policies define the appropriate and prohibited use of Sullivan County information technology resources by all authorized users. These policies apply to all employees, elected officials, contractors, consultants, and any other individuals granted access to County systems, networks, or data.

All use of County technology resources must comply with applicable County policies, standards, and procedures.

Use of artificial intelligence (AI) systems and tools must comply with SCITS-7030.002 Policy – Use of Artificial Intelligence (AI) in County Operations.

SCITS-6000.001 Policy – Acceptable Use of Email

Title	Number
Acceptable Use of Email	SCITS-6000.001
Creation Date: May 2026	
Modified Date:	

Purpose

Electronic mail (e-mail) is a critical and official communication tool of Sullivan County and is used to conduct County business, support operations, and communicate with internal and external stakeholders. As such, e-mail systems and services are County-owned resources and must be used in a secure, responsible, lawful, and professional manner consistent with the mission and obligations of Sullivan County government.

Use of County e-mail systems is a privilege, not a right, and is subject to all applicable County policies, standards, procedures, and legal requirements. Users are expected to exercise sound judgment and professionalism in all communications and to ensure that their use of e-mail does not expose the County to security risk, legal liability, operational disruption, or reputational harm.

Sullivan County is committed to maintaining a workplace that is respectful, professional, and free from harassment, discrimination, and inappropriate conduct. The use of e-mail systems in any manner that is disruptive, offensive, inappropriate, or harmful to individuals or workplace morale is strictly prohibited.

The purpose of this policy is to define acceptable and unacceptable uses of County e-mail systems and services, establish user responsibilities, support compliance with applicable laws and policies, and reduce risks associated with misuse, data exposure, and cybersecurity threats.

Scope

This policy applies to:

- All e-mail systems, services, and platforms owned, licensed, or provided by Sullivan County;
- All users of County e-mail systems, including employees, elected officials, contractors, consultants, vendors, interns, volunteers, and other authorized individuals;
- All e-mail communications and records created, received, stored, transmitted, or managed using County systems or on behalf of the County; and

- Any device, whether County-owned or personally owned, used to access County e-mail systems or County information.

This policy applies regardless of physical location or method of access.

General Policy

County-issued e-mail accounts shall be the official and primary method for conducting County business. Only County-approved e-mail systems and services shall be used for County communications.

Access to personal e-mail services (such as Gmail, Yahoo, or similar platforms) from County-owned devices or from devices connected to the County network may be restricted or prohibited by Information Technology Services based on security risk. Exceptions may be granted on a case-by-case basis with approval from the Chief Information Officer (CIO) or designee.

The County reserves the right to implement technical controls, including blocking, filtering, monitoring, and conditional access, to protect County systems and information from cybersecurity threats, including but not limited to phishing, malware, ransomware, and data exfiltration.

Each authorized user shall be assigned an individual e-mail account. Users are responsible for maintaining the confidentiality and security of their account credentials and for all activity conducted under their account.

E-mail accounts are issued based on job function and business need, as determined by the Department Head in coordination with Information Technology Services. Access may also be granted to non-employees, including contractors, interns, volunteers, or partners, where a legitimate business need exists and where appropriate approvals and agreements are in place.

Requests for non-employee e-mail access must be submitted to Information Technology Services and must include appropriate justification and documented approval. All such access shall be governed by written terms and conditions, including acceptable use, security requirements, and termination provisions.

E-mail access shall be terminated promptly upon separation from County service or when no longer required for business purposes. The County is under no obligation to retain, transfer, or provide access to an individual’s e-mail content following termination, except as required for operational, legal, or records retention purposes.

Users are expected to review and respond to e-mail in a timely manner consistent with their job responsibilities. E-mail may be used to distribute important operational, administrative, legal, and emergency communications, and users are responsible for remaining informed.

Users are responsible for managing their mailbox, including organizing, archiving, and deleting messages as appropriate. Mailbox size limits may be enforced to ensure system performance, security, and cost control. Users must comply with such limits and manage their mailboxes accordingly.

Acceptable Use

E-mail systems shall be used primarily for official County business. Acceptable uses include, but are not limited to:

- Communicating with County employees, departments, vendors, partners, and members of the public in support of official duties;
- Sharing information necessary to perform assigned responsibilities;
- Coordinating operations, projects, and services; and
- Participating in training, professional development, or other work-related activities.

Limited incidental personal use is permitted provided that such use:

- Does not interfere with job performance or County operations;
- Does not consume more than minimal system resources;
- Does not violate any County policy, law, or ethical standard; and
- Does not expose the County to security, legal, or reputational risk.

Prohibited Use

Use of non-County email systems for conducting County business is prohibited unless explicitly authorized.

The following activities are strictly prohibited when using County e-mail systems or services:

- Use for any unlawful, fraudulent, or malicious purpose, including but not limited to harassment, discrimination, defamation, copyright infringement, or unauthorized access;
- Sending, receiving, or storing content that is obscene, threatening, harassing, discriminatory, or otherwise inappropriate in a professional workplace;
- Use of e-mail to solicit for personal commercial gain, political campaigning, or unauthorized fundraising activities, except as expressly authorized by the County;
- Sharing account credentials or using another individual’s account;
- Attempting to bypass security controls or access restrictions;
- Opening, forwarding, or distributing suspicious or malicious attachments, links, or messages;
- Sending excessively large attachments or engaging in behavior that degrades system performance;
- Unauthorized access to, alteration of, or deletion of e-mail or files belonging to another user or the County;
- Distribution of chain letters, spam, or unsolicited mass communications not related to County business; and

- Any use that violates County policy, administrative directive, contractual obligation, or applicable law.

Users shall exercise caution when interacting with e-mail content, particularly messages from unknown or unexpected sources, as e-mail remains a primary vector for cybersecurity threats.

Security and Records Management

All e-mail communications created, received, or stored through County systems are considered official County records and may be subject to records retention requirements, audit, legal discovery, subpoena, or disclosure under applicable law, including the Freedom of Information Law (FOIL).

Users must ensure that e-mail communications are accurate, appropriate, professional, and consistent with County obligations as a public entity.

The County reserves the right, subject to applicable law and due process, to monitor, access, review, retrieve, and disclose e-mail communications and related records for legitimate governmental purposes, including system administration, security monitoring, investigation, audit, legal compliance, and operational needs.

While the County does not routinely monitor the content of user communications, e-mail messages may be accessed in the normal course of system administration or in response to security events, legal requirements, or policy violations.

Backup and archival copies of e-mail messages may exist even after user deletion, in accordance with County retention and recovery practices.

Users should exercise extreme caution when transmitting confidential or sensitive information via e-mail. Where appropriate, additional safeguards such as encryption or secure file transfer methods should be used.

Monitoring and Enforcement

E-mail systems and services are the property of Sullivan County. The County may implement monitoring, filtering, logging, and other controls to ensure the security, integrity, and proper use of its systems.

If misuse, policy violation, or suspicious activity is detected or reasonably suspected, the County may review and use e-mail records in accordance with applicable law and established procedures.

Where appropriate and practicable, reasonable efforts may be made to notify affected users; however, such notice may not be provided in all circumstances.

Enforcement actions shall be administered in accordance with applicable personnel policies, collective bargaining agreements, and legal requirements.

Reporting Requirements

Any suspected misuse of e-mail systems, phishing attempt, security incident, inappropriate message, or policy violation shall be reported immediately to a supervisor, Department Head, Information Technology Services, or the Chief Information Officer (CIO).

Users who receive suspicious or offensive e-mail messages shall not forward, delete, or respond to such messages unless directed to do so by Information Technology Services. Such messages should be reported promptly for review and response.

Disclaimer and Liability

Sullivan County assumes no liability for direct or indirect damages arising from a user's improper or unauthorized use of County e-mail systems or services, except as otherwise required by law.

Users are solely responsible for the content they create, transmit, or distribute using County systems. The County is not responsible for third-party claims arising from unauthorized, unlawful, or improper use of its e-mail systems or services.

SCITS-6010.001 Policy – Acceptable Use of Internet and Online Services Policy

Title	Number
Acceptable Use of Internet and Online Services Policy	**SCITS-6010.001**
Creation Date: **May 2026**	
Modified Date:	

Purpose

Internet access and online services are critical tools supporting the operations of Sullivan County government, including communication, research, service delivery, collaboration, and access to cloud-based systems and applications.

The purpose of this policy is to define acceptable and unacceptable use of Sullivan County Internet resources and online services, including web browsing, electronic communications, cloud applications, file transfers, social media, streaming services, and voice or video communications conducted over Internet-based platforms.

This policy is intended to promote appropriate use, protect County systems and data from cybersecurity threats, ensure compliance with applicable laws and policies, preserve network performance, and maintain the integrity and reputation of Sullivan County.

Scope

This policy applies to:

- All Internet access provided by or through Sullivan County systems, networks, or services;
- All users of County Internet resources, including employees, elected officials, contractors, consultants, vendors, interns, volunteers, and other authorized individuals;
- All devices used to access County Internet services, whether County-owned or personally owned; and
- All activities conducted using County Internet access, including browsing, communications, file transfers, and use of web-based applications or services.

Internet access is provided through individually assigned user accounts and authentication credentials. Department Heads are responsible for ensuring that access is appropriate to job function and business need, in coordination with Information Technology Services.

General Policy

Internet resources shall be used primarily for official County business purposes in a secure, responsible, and professional manner.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has authority to establish, enforce, and modify Internet access controls, including monitoring, filtering, blocking, and restriction of access to websites, services, applications, or content that present security, legal, operational, or reputational risk.

Use of the Internet through County systems must comply with all applicable federal and New York State laws, County policies, administrative directives, contractual obligations, and ethical standards.

Users are responsible for ensuring that their use of Internet resources does not expose the County to cybersecurity threats, legal liability, operational disruption, or reputational harm.

Acceptable Use

Users are encouraged to use Internet resources to support the goals and objectives of Sullivan County. Acceptable uses include, but are not limited to:

- Communicating with County employees, departments, vendors, partners, and the public in support of official duties;
- Accessing information, resources, or services necessary to perform assigned job responsibilities;
- Conducting research, analysis, or data gathering relevant to County operations;
- Participating in training, education, or professional development activities; and
- Utilizing approved cloud-based or web-based applications for County business purposes.

Limited personal use is permitted provided that such use:

- Is minimal and does not interfere with job performance or County operations;
- Does not consume excessive network resources;
- Does not violate any County policy, law, or ethical obligation; and
- Does not introduce security, legal, or reputational risk.

Prohibited Use

The following activities are strictly prohibited when using County Internet resources:

- Use for any unlawful, fraudulent, or malicious purpose, including but not limited to copyright infringement, harassment, defamation, fraud, identity theft, or unauthorized system access;
- Accessing, transmitting, or distributing content that is obscene, pornographic, threatening, discriminatory, or otherwise inappropriate in a professional workplace;
- Use of Internet resources in a manner that violates County policies, administrative directives, or contractual obligations;
- Misrepresentation of Sullivan County, including unauthorized representation in online communications or platforms;
- Engaging in personal commercial activity, political campaigning, unauthorized solicitation, or dissemination of chain letters;
- Establishing or participating in unauthorized peer-to-peer networks or file-sharing services;
- Downloading, installing, or using unauthorized software, applications, or browser extensions;
- Attempting to bypass or circumvent security controls, filtering mechanisms, or monitoring systems;
- Accessing, copying, altering, or deleting County or third-party data without authorization;
- Streaming audio or video content, or using Internet services in a manner that consumes excessive bandwidth and interferes with business operations, unless required for legitimate County purposes; and
- Using non-approved devices, applications, or services for voice, video, or data communications without authorization.

Users must exercise caution when accessing external websites, downloading files, or interacting with unknown or untrusted sources, as these activities are common vectors for malware, phishing, and other cyber threats.

Security Requirements

Users shall protect their authentication credentials and shall not share account or password information with others. Internet access accounts are to be used only by the assigned user for authorized purposes.

Users must take reasonable precautions to prevent unauthorized access to County systems, including:

- Logging out of systems when not in use;
- Securing devices used to access County resources;
- Avoiding access to suspicious or untrusted websites;
- Not downloading or executing files from unknown or unverified sources; and
- Reporting suspected phishing attempts or malicious activity.

If a user believes that their account credentials have been compromised, they must immediately notify Information Technology Services and request a password reset.

Monitoring, Filtering, and Records

All Internet activity conducted through County systems may be monitored, logged, filtered, and reviewed by Sullivan County for legitimate governmental purposes, including system administration, cybersecurity protection, audit, investigation, legal compliance, and operational oversight.

The County utilizes filtering and security tools to restrict access to websites and services that are deemed unsafe, inappropriate, or not related to County business. The CIO, or designee, may modify filtering and access controls as necessary to address evolving risks and operational needs.

All data transmitted through County systems, including Internet activity, may constitute official County records and may be subject to retention requirements, audit, subpoena, legal discovery, or disclosure under applicable law, including the Freedom of Information Law (FOIL).

Users are responsible for ensuring that all Internet activity conducted using County systems is accurate, appropriate, lawful, and consistent with County obligations as a public entity.

Disclaimer and Liability

Sullivan County assumes no liability for direct or indirect damages arising from a user's connection to or use of the Internet through County systems, except as otherwise required by law.

The County does not guarantee the accuracy, reliability, or security of information obtained through Internet sources and is not responsible for the content of external websites or services.

Users are solely responsible for the material they access, transmit, or disseminate through the Internet using County systems.

Enforcement

Failure to comply with this policy may result in restriction or revocation of Internet access, disciplinary action, termination of employment or contractual relationship, and/or legal action as appropriate.

Enforcement actions shall be administered in accordance with applicable personnel policies, collective bargaining agreements, and legal requirements.

SCITS-6020.001 Policy – Acceptable Use of Mobile Devices, Wireless Connectivity, and Location Services (BYOD Prohibited)

Title	Number
Policy – Acceptable Use of Mobile Devices, Wireless Connectivity, and Location Services (BYOD Prohibited)	**SCITS-6020.001**

Creation Date: **May 2026**

Modified Date:

Purpose

Mobile devices and wireless connectivity services, including smartphones, tablets, laptops, mobile hotspots, cellular-enabled devices, and location-enabled technologies such as GPS, are essential tools supporting the operations of Sullivan County government.

These resources enable communication, remote work, field operations, emergency response, and access to County systems and data. Due to their portability, exposure to external networks, and increased risk of loss, theft, or compromise, they must be used in a secure, controlled, and accountable manner.

The purpose of this policy is to establish requirements governing the acquisition, configuration, use, security, management, and oversight of mobile devices and associated services in order to protect the confidentiality, integrity, and availability of County systems and information.

Scope

This policy applies to:

- All Sullivan County employees, elected officials, contractors, consultants, vendors, interns, volunteers, and other authorized users;
- All County-issued or County-funded mobile devices, including but not limited to smartphones, tablets, laptops, mobile hotspots, GPS-enabled devices, and wireless communication tools;
- All cellular, wireless data, and location-based services associated with such devices; and
- Any device used to access, store, transmit, or process County systems or data.

Use of any device to access County systems or data is a privilege, not a right, and is subject to approval, monitoring, and compliance with this policy and all related County requirements.

Bring Your Own Device (BYOD) – Prohibited

The use of personally owned devices (Bring Your Own Device – BYOD) to access, store, transmit, or process Sullivan County systems, networks, applications, or data is strictly prohibited.

No employee, contractor, or authorized user shall:

- Access County systems or data from a personally owned device;
- Store County data on a personally owned device; or
- Use personal devices as a substitute for County-issued equipment for official business purposes.

Information Technology Services will not approve, support, or configure personally owned devices for access to County systems under any circumstances.

Any attempt to access County systems using a non-County-issued or unapproved device will be blocked and may result in disciplinary action.

General Policy

All mobile devices, wireless connectivity services, and associated accounts provided by Sullivan County are County property or are managed on its behalf and are intended for official business use.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, retains authority over the selection, approval, configuration, security, deployment, monitoring, and lifecycle management of all mobile devices and related services.

All mobile device access to County systems must:

- Be conducted only from County-issued and Information Technology Services-approved devices;
- Be approved in advance by Information Technology Services; and
- Comply with all County security and management requirements.

Information Technology Services retains sole discretion to approve, deny, restrict, or revoke mobile device access as necessary to protect County systems, data, and operations.

Device Management and Security Requirements

All mobile devices authorized to access County systems or data must be enrolled in and managed through the County's Mobile Device Management (MDM) platform, as designated by Information Technology Services.

Security controls may include, but are not limited to:

- Device encryption;
- Authentication requirements (PIN, password, or biometric controls);
- Remote lock and remote wipe capabilities;
- Application control and restriction;
- Configuration management and enforcement;
- Compliance monitoring; and
- Conditional access controls.

Users shall not disable, bypass, or interfere with device management, security controls, or monitoring systems.

Devices that are noncompliant, insecure, or present a risk to County systems may be restricted, quarantined, or blocked from access without prior notice.

Endpoint and Operational Requirements

All County-issued mobile and computing devices must be maintained in a secure, compliant, and operational state.

Users must:

- Maintain physical control of devices and prevent unauthorized access;
- Lock devices when unattended;
- Ensure devices are not modified, jailbroken, or used with unapproved software;
- Use only County-approved methods for storing, transmitting, or accessing County data; and
- Immediately report lost, stolen, or compromised devices.

To maintain security and functionality:

- Devices must connect to the Internet regularly to receive updates, patches, and security controls;
- Devices authenticated with a County Network ID must periodically connect to the County network to maintain system integrity and access; and
- Required security tools (e.g., antivirus, endpoint protection, VPN, MDM) must remain enabled and operational at all times.

Failure to maintain compliance may result in restricted or revoked access.

Acceptable Use

County-issued mobile devices and services shall be used primarily for official business purposes, including:

- Communication and coordination of County operations;
- Access to County systems, applications, and data;
- Fieldwork, inspections, and emergency response; and
- Other duties consistent with assigned responsibilities.

Limited personal use is permitted only when such use:

- Is minimal and incidental;
- Does not interfere with job performance or operations;
- Does not incur unnecessary cost; and
- Does not violate any County policy, law, or ethical standard.

Prohibited Use

The following activities are strictly prohibited:

- Use of personally owned or unapproved devices to access County systems (BYOD);
- Circumventing or disabling security controls or monitoring systems;
- Installing unauthorized applications or software;
- Storing or transmitting County data through unsecured or unauthorized means;
- Use for personal commercial activity, political activity, or unauthorized solicitation;
- Excessive personal use or use that incurs unnecessary cost;
- Accessing, transmitting, or storing unlawful, inappropriate, or offensive content; and
- Any activity that introduces security, legal, or operational risk to the County.

Wireless Connectivity, Location Services, and Safety

Wireless access to County systems must occur only through secure, County-approved methods.

Location services and tracking capabilities may be enabled and managed by the County for legitimate operational, security, asset management, or emergency response purposes. Users shall not disable such controls where required.

Employees shall not use mobile devices in a manner that is unsafe or violates applicable law, including while operating vehicles or equipment, except where authorized for emergency response.

Cost Control and Oversight

Users shall utilize mobile devices and services in a cost-conscious and responsible manner.

- International or out-of-region use must be coordinated in advance with Information Technology Services;
- The County may implement controls, limitations, or service adjustments to manage cost and risk; and

- Departments are responsible for overseeing usage, cost, and compliance within their areas.

User Responsibilities

Users are responsible for:

- Protecting County devices and data from unauthorized access or disclosure;
- Maintaining compliance with all security requirements;
- Reporting loss, theft, misuse, or security incidents immediately;
- Using devices in a professional, lawful, and secure manner; and
- Complying with all directives issued by Information Technology Services.

Lost, Stolen, or Compromised Devices

Users must immediately report any lost, stolen, or compromised device.

The County reserves the right to remotely lock, locate, or wipe devices to protect County data. Devices must be inspected and reauthorized before being returned to service.

Monitoring and Enforcement

Sullivan County reserves the right, subject to applicable law, to monitor, manage, access, and review:

- Device usage;
- Communications;
- System access; and
- Location data, where applicable.

Failure to comply with this policy may result in:

- Suspension or revocation of access;
- Disciplinary action; and/or
- Legal action where appropriate.

Enforcement actions shall be administered in accordance with applicable personnel policies, collective bargaining agreements, and legal requirements.

Disclaimer and Liability

Nothing in this policy shall be construed to limit or supersede any rights or obligations of Sullivan County under applicable law.

To the extent permitted by law, Sullivan County shall not be liable for damages arising from the improper, unauthorized, or unlawful use of mobile devices or services.

Users are responsible for their use of County-issued devices and for complying with all applicable policies, laws, and requirements.

SCITS-6030.001 Policy – Telephony and Unified Communications Policy

Title	Number
Telephony and Unified Communications Policy	**SCITS-6030.001**
Creation Date: **May 2026**	
Modified Date:	

Purpose

Telephone and voice communication services, including traditional telephony, Voice over IP (VoIP), voicemail, fax services, softphone applications, and mobile-integrated communication platforms, are essential tools supporting the daily operations of Sullivan County government.

These services are provided to facilitate official County business, support communication with the public and partner agencies, and enable efficient internal coordination. As County-owned or County-managed resources, telephony and communication systems must be used in a secure, responsible, cost-effective, and professional manner consistent with the mission and obligations of Sullivan County.

The purpose of this policy is to establish requirements for the appropriate use, management, security, and oversight of County telephony and communication services, while balancing operational needs, cost control, cybersecurity risk, and legal compliance.

Scope

This policy applies to:

- All telephony, voicemail, fax, and unified communication systems and services owned, leased, licensed, or provided by Sullivan County;
- All devices used to access such services, including desk phones, mobile devices, softphones, and computer-based communication tools;
- All employees, elected officials, contractors, consultants, vendors, interns, volunteers, and other authorized users of County communication systems; and

- All voice communications, voicemail messages, call records, and related data created, transmitted, received, or stored using County systems or on behalf of the County.

This policy applies regardless of device ownership or physical location of use.

General Policy

All County telephony and communication systems, equipment, accounts, voicemail boxes, and associated data are the property of Sullivan County and are provided for the conduct of official business.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has authority over the administration, configuration, security, and operational control of County telephony and unified communications systems, except where specific operational authority is assigned by law or formal designation (such as public safety dispatch systems).

Information Technology Services is responsible for the implementation, administration, maintenance, and support of County telephony systems, including provisioning, configuration, monitoring, and repair. Departments shall coordinate all requests for installation, modification, or removal of services through established Information Technology Service request procedures.

Department Heads and supervisors are responsible for ensuring that telephony and communication services are used appropriately, efficiently, and in compliance with this policy and for notifying Information Technology Services of personnel or operational changes requiring system updates.

Users shall utilize telephony and communication services in a manner that is cost-effective, operationally appropriate, and consistent with County business needs. Use shall not be excessive, wasteful, or inconsistent with the intended purpose of the service.

Voicemail accounts shall be secured through authentication controls, including PINs or other approved mechanisms. Authentication credentials must be protected and shall not be shared. Security requirements, including credential standards and rotation, may be established and enforced by Information Technology Services.

Voicemail shall be used as a backup communication method when calls cannot be answered. Users are expected to respond to voicemail messages in a timely manner consistent with their job responsibilities.

Users who will be unavailable for extended periods shall update voicemail greetings to reflect their absence and, where appropriate, provide alternate contact information.

Use of fee-based services, such as directory assistance or premium calling services, should be avoided unless necessary for legitimate County business purposes.

Acceptable Use

County telephony and communication systems shall be used primarily for official business purposes, including:

- Communicating with County employees, departments, public agencies, vendors, and members of the public;
- Supporting service delivery, emergency response, and operational coordination;
- Conducting official meetings, notifications, and administrative communications; and
- Facilitating business processes and customer service functions.

Limited personal use is permitted provided that such use:

- Is brief and infrequent;
- Does not interfere with job performance or County operations;
- Does not incur unnecessary cost to the County;
- Does not violate any County policy, law, or ethical obligation; and
- Does not expose the County to security, legal, or reputational risk.

Prohibited Use

The following uses of County telephony and communication systems are strictly prohibited:

- Use for any unlawful, fraudulent, or malicious purpose;
- Transmission of obscene, threatening, harassing, discriminatory, or otherwise inappropriate communications;
- Unauthorized access to telephony systems, voicemail accounts, or call records;
- Use of another individual's account or credentials without authorization;
- Attempting to bypass system controls, security mechanisms, or billing safeguards;
- Use for personal commercial activity, political campaigning, or unauthorized solicitation;
- Use of premium-rate services (such as 1-900 numbers) or other fee-based services not required for County business;
- Excessive or abusive personal use;
- Any use that violates County policy, administrative directive, contractual obligation, or applicable law.

Misuse of telephony or communication systems may result in disciplinary action, up to and including termination, as well as potential legal or financial consequences.

Cost Control and Accountability

Users are expected to use telephony services in a cost-conscious manner. Calls, messaging, and communication services should be limited to what is necessary for effective conduct of County business.

Personal long-distance or chargeable communications should not be billed to the County unless necessary and approved by a supervisor. Where such use occurs, the user may be required to reimburse the County in accordance with established procedures.

Information Technology Services may implement controls, reporting, or restrictions to manage costs, including call detail monitoring, service limitations, or usage thresholds.

Security and Records Management

Voice communications, voicemail messages, call logs, and related data generated through County systems may constitute official County records and may be subject to records retention requirements, audit, legal discovery, subpoena, or disclosure under applicable law, including the Freedom of Information Law (FOIL).

Users shall ensure that communications conducted using County systems are professional, appropriate, and consistent with County obligations as a public entity.

Users should exercise caution when communicating sensitive or confidential information via telephony or voicemail. Where appropriate, alternative secure communication methods should be used.

Monitoring and Oversight

Sullivan County reserves the right, subject to applicable law and due process, to monitor, access, review, and retrieve telephony usage, voicemail content, and related records for legitimate governmental purposes, including system administration, service quality assurance, troubleshooting, security monitoring, investigation, audit, and legal compliance.

Monitoring shall be conducted in a manner consistent with applicable law, policy, and operational necessity. While routine monitoring of content is not conducted in all cases, access may occur in the normal course of system administration or in response to incidents, investigations, or operational needs.

Service Requests and Support

All requests for telephony services, including installation, changes, moves, or disconnections, shall be submitted through the County's designated Information Technology Service request process.

Users shall report service issues, outages, or suspected problems promptly to Information Technology Services through established support channels.

Information Technology Services shall establish reasonable service timelines and priorities based on operational need, resource availability, and system impact.

Reporting Misuse or Security Concerns

Any suspected misuse of telephony systems, unauthorized access, suspicious activity, or policy violation shall be reported immediately to a supervisor, Department Head, Information Technology Services, or the Chief Information Officer (CIO).

Disclaimer and Liability

Sullivan County assumes no liability for direct or indirect damages arising from improper or unauthorized use of County telephony or communication systems, except as otherwise required by law.

Users are responsible for the content of their communications. The County is not responsible for third-party claims arising from unauthorized, unlawful, or improper use of its communication systems.

SCITS-6040.001 Policy – Acceptable Use of Social Media and Online Platforms

Title	Number
Acceptable Use of Social Media and Online Platforms	**SCITS-6040.001**

Creation Date: **May 2026**

Modified Date:

Purpose

Social media and online platforms—including social networking sites, blogs, forums, content-sharing platforms, and other Web-based communication tools—can support Sullivan County's mission by enabling communication, outreach, transparency, and public engagement.

However, improper or unmanaged use of such platforms may create cybersecurity risks, legal exposure, reputational harm, operational disruption, and potential violations of confidentiality, privacy, and public records requirements.

The purpose of this policy is to establish standards for the appropriate, responsible, and lawful use of social media and online platforms, and to define expectations for both official County use and personal use where such use may impact Sullivan County.

Nothing in this policy is intended to limit or interfere with employee rights under applicable law, including rights protected under Section 7 of the National Labor Relations Act.

Scope

This policy applies to:

- All social media and online platforms, including but not limited to Facebook, X (formerly Twitter), Instagram, LinkedIn, blogs, forums, video platforms, and emerging technologies;
- All County employees, elected officials, contractors, consultants, vendors, interns, volunteers, and other authorized users;
- All use of social media conducted using County devices, networks, systems, or accounts; and
- Personal use of social media where such activity references, relates to, or may reasonably impact Sullivan County, its operations, employees, residents, or reputation.

Users are responsible for all online activities conducted using County systems or associated with their County role.

General Policy

Use of social media on behalf of Sullivan County is restricted to authorized accounts and authorized personnel.

The Commissioner of Information Technology / Chief Information Officer (CIO), in coordination with County leadership and designated departments, has authority over the security, access, and technical management of County social media platforms.

Departments may establish official social media accounts only with appropriate authorization and in accordance with County communication, records retention, and security requirements.

Employees are prohibited from creating, maintaining, or representing unauthorized social media accounts or profiles on behalf of Sullivan County.

Official County business shall not be conducted through personal social media accounts. All official communications must be conducted through authorized County communication channels, including official email systems or approved County-managed platforms.

Access to social media platforms from County systems may be restricted, monitored, or limited based on operational need, security risk, and business justification.

Official Use of Social Media

Authorized users managing official County social media accounts shall:

- Ensure that all content is accurate, professional, and consistent with County policies and messaging;
- Comply with all applicable laws, including public records, accessibility, and records retention requirements;
- Protect confidential, sensitive, and restricted information;
- Use only approved accounts, devices, and access methods;
- Coordinate with appropriate County leadership when publishing official statements or information; and
- Maintain appropriate security controls, including account protection and credential management.

All content published through official County accounts may constitute public records and may be subject to retention, disclosure, audit, or legal review.

Personal Use of Social Media

Sullivan County recognizes that employees may engage in personal use of social media on their own time. However, such use is not private and may have implications for the employee and the County, particularly where County affiliation is identified, known, or reasonably inferred.

Employees are responsible for their online conduct and must ensure that personal use of social media does not:

- Interfere with job performance or County operations;
- Violate County policies, including codes of conduct, confidentiality, and acceptable use policies;
- Disclose confidential, proprietary, or legally protected information;
- Create a hostile, discriminatory, or unprofessional work environment; or
- Damage the reputation, credibility, or operational effectiveness of Sullivan County.

Employees should be aware that they may be perceived as representatives of the County, even when acting in a personal capacity.

Legal and Professional Responsibility

Individuals are legally responsible for content they publish or share on social media platforms. Users may be held liable for content that is defamatory, obscene, discriminatory, infringing, or otherwise unlawful.

Employees shall exercise sound judgment and professionalism in all online communications and should avoid:

- Posting inaccurate or misleading information;
- Using offensive, derogatory, or inflammatory language;
- Making unauthorized legal or policy interpretations;
- Sharing copyrighted or protected material without authorization; or
- Making statements that could reasonably be interpreted as official County positions without authorization.

Participation in social media is undertaken at the user's own risk.

Confidentiality and Privacy

Under no circumstances shall employees post, share, or disclose confidential, proprietary, sensitive, or legally protected information related to Sullivan County or any individual associated with the County.

This includes, but is not limited to:

- Personally identifiable information (PII), protected personal or sensitive information (PPSI), protected health information (PHI), or payment card information (PCI);

- Information related to County operations, investigations, systems, or internal processes not intended for public release;
- Information about residents, clients, program participants, employees, or partners that is protected by law or policy; and
- Any information restricted under HIPAA, HITECH, CJIS, or other applicable laws or regulations.

Unauthorized disclosure of such information may result in disciplinary action, legal liability, and regulatory consequences.

County logos, branding, and official identifiers shall not be used on personal social media accounts without authorization.

Guidelines for Responsible Use

Employees who engage in social media use are expected to adhere to the following guidelines:

- Be accurate, truthful, and respectful in all communications;
- Avoid content that could be perceived as discriminatory, harassing, or offensive based on protected characteristics;
- Clearly distinguish personal opinions from official County positions;
- Use disclaimers where appropriate, such as:
  "The views expressed are my own and do not represent the views of Sullivan County."
- Exercise caution when discussing topics related to County operations or personnel;
- Consider the potential impact of posts on colleagues, the public, and the County's reputation; and
- Comply with all applicable County policies and legal requirements.

Employees are encouraged to use good judgment and to seek guidance from supervisors or appropriate County officials when uncertain.

Monitoring and Enforcement

Sullivan County reserves the right, subject to applicable law, to monitor publicly available social media activity where it relates to County operations, systems, or policy compliance.

Use of social media on County systems or accounts may be monitored, logged, or restricted for security, operational, or compliance purposes.

Violations of this policy may result in disciplinary action, up to and including termination of employment, as well as potential legal action where applicable.

Enforcement actions shall be administered in accordance with applicable personnel policies, collective bargaining agreements, and legal requirements.

Reporting Concerns

Any suspected misuse of social media, unauthorized account activity, disclosure of confidential information, or other policy violations shall be reported promptly to a supervisor, Department Head, Information Technology Services, or the Chief Information Officer (CIO).

Disclaimer

Sullivan County assumes no liability for direct or indirect damages arising from an individual's personal use of social media platforms, except as otherwise required by law.

Users are solely responsible for the content they publish or disseminate. The County is not responsible for third-party claims arising from unauthorized or improper use of social media.

SCITS-6050.001 Policy – Acceptable Use of Cloud Services & Storage

Title	Number
Acceptable Use of Cloud Storage & Services	**SCITS-6050.001**

Creation Date: **May 2026**

Modified Date:

Purpose

Cloud storage and cloud-based services—including Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and other externally hosted solutions—are widely used to store, process, transmit, and share data.

While such services may offer operational benefits, their use introduces significant risks related to data security, privacy, legal compliance, vendor management, and unauthorized data exposure.

The purpose of this policy is to establish requirements governing the evaluation, approval, access, and use of cloud storage and cloud-based services to ensure that Sullivan County data is protected and that all such services are implemented in a secure, compliant, and controlled manner.

Scope

This policy applies to:

- All Sullivan County employees, elected officials, contractors, consultants, vendors, interns, and other authorized users;
- All County data, regardless of format or classification;
- All cloud storage and cloud-based services used to store, process, transmit, or access County data; and
- All devices, systems, or applications used to access such services, whether County-owned or personally owned.

This policy applies to all external cloud services, including but not limited to document storage platforms, file-sharing systems, collaboration tools, hosted applications, and externally managed infrastructure.

Personal cloud storage accounts shall not be used for County business.

General Policy

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has sole authority over the evaluation, approval, implementation, and use of all cloud storage and cloud-based services involving County data or systems.

No employee, department, or third party shall procure, subscribe to, access, or use any cloud service for County business purposes without prior written approval from Information Technology Services.

All proposed cloud services must undergo appropriate review and approval processes, including, but not limited to:

- Information Technology security and architecture review;
- Procurement and contractual review;
- Legal review by the County Attorney, where applicable; and
- Compliance review for applicable laws and regulations.

Unauthorized use of cloud services for the storage, transmission, processing, or exchange of County data is strictly prohibited.

Approved Methods for File Sharing and Data Exchange

Sullivan County provides approved, secure methods for file sharing and external data exchange.

Where file sharing or external collaboration is required, users shall utilize County-provided and approved solutions, including the County's **on-premises ShareFile system**, or other solutions expressly approved by Information Technology Services.

Use of external or third-party cloud storage services for file sharing is prohibited unless explicitly approved in writing by Information Technology Services.

Data Security and Compliance

All use of cloud services must comply with:

- Applicable federal and New York State laws;
- County policies and standards;
- Data protection and privacy requirements; and
- Regulatory obligations, including but not limited to HIPAA, HITECH, CJIS, PCI-DSS, and other applicable frameworks.

The CIO, or designee, shall determine what types of data, if any, may be stored or processed in approved cloud environments based on risk, classification, and legal requirements.

Under no circumstances shall confidential, sensitive, or regulated data be stored, transmitted, or processed in any cloud service that has not been formally approved.

User Responsibilities

Users are responsible for:

- Using only approved cloud services for County business;
- Protecting County data from unauthorized access or disclosure;
- Not uploading, storing, or sharing County data in unauthorized systems;
- Not creating or using unauthorized cloud service accounts for County business;
- Not accepting terms of service, licenses, or agreements on behalf of the County without proper authorization; and
- Reporting any unauthorized use, suspected data exposure, or security concern immediately.

Users shall not share account credentials or access information for any approved system except as authorized and managed through official processes.

Prohibited Activities

The following activities are strictly prohibited:

- Creating or using personal or unauthorized cloud storage accounts for County business;
- Uploading or transferring County data to unapproved cloud services;
- Entering into cloud service agreements, licenses, or subscriptions without authorization;
- Synchronizing County data to unauthorized external systems or devices;
- Circumventing County security controls or monitoring mechanisms;
- Downloading data from unapproved cloud services onto County systems or networks; and
- Any activity that exposes County systems or data to cybersecurity risk.

Unauthorized cloud usage may introduce risks including ransomware, malware infection, data loss, unauthorized disclosure, and legal liability.

Security Controls

Information Technology Services shall implement appropriate technical controls to:

- Monitor and restrict access to unauthorized cloud services;
- Enforce data protection requirements;
- Prevent unauthorized data transfer or synchronization;
- Detect and respond to potential threats; and
- Ensure compliance with this policy.

Devices, accounts, or users found to be in violation of this policy may be restricted, blocked, or subject to corrective action.

Monitoring and Enforcement

Sullivan County reserves the right, subject to applicable law, to monitor, log, and review access to cloud services and related data activity conducted through County systems or networks.

Violations of this policy may result in:

- Immediate suspension or revocation of system access;
- Removal of unauthorized services or data;
- Disciplinary action, up to and including termination; and/or
- Legal action where applicable.

Enforcement actions shall be administered in accordance with applicable personnel policies, collective bargaining agreements, and legal requirements.

Reporting Requirements

Any suspected unauthorized use of cloud services, data exposure, security incident, or policy violation shall be reported immediately to a supervisor, Department Head, Information Technology Services, or the Chief Information Officer (CIO).

Disclaimer

Sullivan County assumes no liability for direct or indirect damages arising from the unauthorized or improper use of cloud services.

Users are solely responsible for ensuring that their actions comply with this policy and all applicable County requirements.

SCITS-6060.001 Policy – Acceptable Use of Printing, Copying, and Document Output Devices

Title	Number
Acceptable Use of Printing, Copying, and Document Output Devices	**SCITS-6060.001**

Creation Date: **May 2026**

Modified Date:

Purpose

Printing, copying, and document output devices—including printers, copiers, multifunction devices (MFDs), and related services—represent a significant operational and financial investment for Sullivan County.

These resources support the creation, distribution, and management of County records and communications. However, unmanaged or excessive use can result in unnecessary costs, inefficiencies, security risks, and environmental impact.

The purpose of this policy is to establish standards for the appropriate, efficient, secure, and cost-effective use of County printing and copying resources, while promoting responsible consumption of materials such as paper, toner, and ink.

Scope

This policy applies to:

- All printing, copying, scanning, and document output devices owned, leased, licensed, or provided by Sullivan County;
- All employees, elected officials, contractors, consultants, vendors, interns, volunteers, and other authorized users of such equipment; and
- All documents and materials printed, copied, or otherwise produced using County equipment.

General Policy

All printing and copying equipment and services are County resources and shall be used primarily for official County business purposes.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has authority over the selection, deployment, configuration, management, and support of all County printing and document output devices.

Information Technology Services, in coordination with Central Services or other designated departments, shall manage the procurement, deployment, maintenance, and support of printing and copying equipment to ensure standardization, cost control, and operational efficiency.

Users are expected to use printing and copying resources in a manner that is necessary, appropriate, cost-effective, and consistent with County business needs.

Acceptable Use

Printing and copying devices shall be used for documents and materials directly related to the performance of official County duties.

Users are encouraged to minimize printing by utilizing digital workflows, document management systems, and electronic communication methods whenever feasible.

Limited personal use is discouraged and, where permitted, must be minimal, infrequent, and must not result in measurable cost, waste, or interference with County operations.

Cost Control and Efficiency

Users shall take reasonable steps to reduce unnecessary printing and copying and to promote efficient use of resources, including:

- Avoiding the printing of documents unless necessary;
- Utilizing duplex (double-sided) printing where available;
- Using draft or lower-resolution settings when high-quality output is not required;
- Printing multiple pages per sheet where appropriate;
- Using shared networked printers or multifunction devices instead of individual desktop printers;
- Printing only the number of copies required; and
- Avoiding printing documents solely for review or convenience when electronic alternatives are available.

Color printing should be used only when necessary for business purposes, as it typically incurs higher costs than standard monochrome printing.

Large print jobs should be planned and managed to avoid disruption to shared devices and to ensure that output is collected promptly.

Device Management and Restrictions

Installation or use of personal or non-standard printers is generally prohibited due to cost, support, and security considerations. Exceptions may be granted by Information Technology Services where justified by business need, such as confidentiality requirements, remote locations, or operational necessity.

Users shall not install, configure, or connect unauthorized printing devices to the County network without prior approval from Information Technology Services.

Certain paper types or specialty materials may not be compatible with all devices. Users must consult Information Technology Services or designated support personnel before using specialty media such as labels, card stock, transparencies, or other non-standard materials.

Printer and copier supplies, including paper and toner, shall be obtained through approved County channels.

Security and Document Handling

Printed and copied materials may contain sensitive or confidential information. Users are responsible for:

- Promptly retrieving printed documents from shared devices;
- Properly securing documents containing sensitive information;
- Disposing of unwanted documents using appropriate recycling or secure destruction methods; and
- Ensuring that confidential information is not left unattended on output trays or accessible to unauthorized individuals.

Users shall comply with all County data classification, confidentiality, and records management requirements when printing or copying documents.

Prohibited Use

The following activities are prohibited:

- Printing or copying documents unrelated to County business beyond minimal incidental use;
- Excessive or wasteful printing or copying;
- Unauthorized installation or use of personal printing devices;
- Printing, copying, or distributing inappropriate, offensive, or prohibited materials;
- Using devices in a manner that interferes with others' ability to perform their work; and
- Any use that violates County policy, administrative directive, contractual obligation, or applicable law.

Support and Maintenance

Users shall report any malfunction, supply issue, or operational problem with printing or copying equipment to Information Technology Services or the designated support channel promptly.

Users should not attempt to repair, modify, or service equipment unless authorized and trained to do so.

Information Technology Services shall coordinate maintenance, repair, and support activities to ensure device reliability and performance.

Monitoring and Oversight

Sullivan County may monitor usage of printing and copying devices, including print volumes, usage patterns, and associated costs, for purposes of cost control, operational efficiency, audit, and compliance.

Department Heads, in coordination with Information Technology Services, are responsible for reviewing usage within their departments and addressing any misuse or inefficiency.

Enforcement

Failure to comply with this policy may result in restriction of access to printing resources, recovery of costs where appropriate, disciplinary action, and/or other corrective measures in accordance with County policy.

Enforcement actions shall be administered in accordance with applicable personnel policies, collective bargaining agreements, and legal requirements.

Disclaimer

Sullivan County assumes no liability for direct or indirect damages arising from improper or unauthorized use of printing and copying equipment, except as otherwise required by law.

Section 7 — System and Application Security (7000 Series)

SCITS-7000.001 Policy – Software Installation and Application Control

Title	Number
Software Installation and Application Control	**SCITS-7000.001**
Creation Date: May 2026	
Modified Date:	

Purpose

Sullivan County provides standardized, centrally managed technology systems to ensure secure, stable, and efficient operations across all departments.

Uncontrolled installation of software introduces significant risks, including cybersecurity threats, system instability, licensing violations, and increased support complexity.

The purpose of this policy is to establish requirements governing the installation, management, and use of software on County systems to ensure security, compliance, and operational integrity.

Scope

This policy applies to:

- All County-owned or managed devices, including desktops, laptops, tablets, and other computing systems;
- All software, applications, utilities, and executable code installed or used on such devices;
- All users, including employees, elected officials, contractors, consultants, vendors, interns, and other authorized individuals; and
- All systems connected to the Sullivan County network or accessing County resources.

General Policy

All software utilized by any Division, Department, Office, Agency, or Unit of Sullivan County shall be under the control and jurisdiction of the Department of Information Technology Services (ITS), in accordance with duly adopted County Legislature resolutions.

Information Technology Services must be involved in the evaluation, procurement, licensing, installation, renewal, and management of all software used by the County. No department or individual shall independently acquire, install, or utilize software for County business outside of this process.

All software installation and application management on County systems shall be centrally controlled and performed exclusively by Information Technology Services.

End users are not permitted to install, download, or otherwise introduce software onto County systems.

Technical controls, including Group Policy and other endpoint management tools, shall be implemented to prevent unauthorized software installation and execution.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has sole authority over the approval, deployment, configuration, and removal of all software on County systems.

Software Request and Approval

Users requiring software to perform their job duties must submit a request through approved Information Technology Services processes.

All software requests shall be evaluated based on:

- Business need and operational justification;
- Security risk and compatibility with County systems;
- Licensing and legal compliance requirements;
- Supportability and maintenance considerations; and
- Alignment with County technology standards.

Information Technology Services reserves the right to approve or deny any software request.

Approved software shall be installed, configured, and maintained by Information Technology Services.

Application Control and Standardization

Sullivan County maintains a controlled application environment. Software available on County systems is determined by Information Technology Services and may vary based on role, department, and operational requirements.

The County does not maintain or publish a comprehensive list of approved software titles for general distribution. All approved software is provisioned based on authorized requests and operational needs.

Users shall use only software that has been installed and approved by Information Technology Services.

Prohibited Activities

The following activities are strictly prohibited:

- Installing or attempting to install software on County systems without authorization;
- Downloading or executing software from the Internet or other external sources;
- Using personal, unlicensed, or unauthorized software on County systems;
- Circumventing or attempting to bypass technical controls that restrict software installation or execution;
- Using software in violation of licensing agreements or legal requirements; and
- Introducing software that poses a security, operational, or compliance risk.

Licensing and Compliance

All software used on County systems must be properly licensed and used in accordance with applicable agreements, terms, and legal requirements.

Information Technology Services shall manage software licensing, inventory, and compliance.

Unauthorized or unlicensed software is strictly prohibited.

Monitoring and Enforcement

Sullivan County reserves the right, subject to applicable law, to monitor software installation, usage, and system activity to ensure compliance with this policy.

Information Technology Services may:

- Remove or disable unauthorized software without notice;
- Restrict system access where violations occur;
- Conduct periodic audits of software and systems; and
- Implement technical controls to enforce compliance.

Support and Maintenance

Information Technology Services shall provide support only for software that has been approved and installed in accordance with this policy.

The County does not support unauthorized or unapproved software.

Enforcement

Failure to comply with this policy may result in:

- Removal of unauthorized software;
- Restriction or revocation of system access;
- Disciplinary action, up to and including termination; and/or
- Legal action where applicable.

Disclaimer

Sullivan County assumes no liability for damages resulting from unauthorized software installation or use in violation of this policy, except as otherwise required by law.

SCITS-7010.001 Policy – Email Encryption and Secure Messaging

Title	Number
Email Encryption and Secure Messaging	**SCITS-7010.001**
Creation Date: **May 2026**	
Modified Date:	

Purpose

Email is a primary method of communication for Sullivan County and is frequently used to transmit information that may be confidential, sensitive, or regulated.

The purpose of this policy is to ensure that all outbound email communications containing County information are protected through appropriate encryption controls to safeguard confidentiality, integrity, and compliance with applicable laws and regulations.

Sullivan County utilizes automated email encryption to reduce the risk of unauthorized access, data exposure, and non-compliance with legal and regulatory requirements.

Scope

This policy applies to:

- All email communications sent from Sullivan County email systems;
- All employees, elected officials, contractors, consultants, vendors, interns, and other authorized users of County email systems; and
- All data transmitted via email, including attachments and embedded content.

This policy applies to all County-managed email platforms and services.

General Policy

All outbound email messages sent from Sullivan County email systems to external recipients shall be encrypted by default using County-approved encryption technology.

Sullivan County currently utilizes a centrally managed email encryption solution, including **Zix Email Encryption**, or its successor as designated by Information Technology Services.

Encryption is automatically applied and enforced at the system level. Users do not have the ability to disable or bypass encryption for outbound messages.

Use of personal or non-County email accounts to transmit County data, including confidential, sensitive, or regulated information, is strictly prohibited.

Data Protection and Compliance

Email encryption is implemented to protect information including, but not limited to:

- Personally Identifiable Information (PII);
- Personal, Private, or Sensitive Information (PPSI);
- Protected Health Information (PHI);
- Payment Card Information (PCI); and
- Any other data classified as confidential or restricted.

All email communications must comply with applicable laws and regulations, including but not limited to:

- Health Insurance Portability and Accountability Act (HIPAA);
- 42 CFR Part 2 (Substance Use Disorder records);
- New York State privacy and security laws; and
- Any other applicable federal, state, or contractual requirements.

Where stricter regulatory requirements apply, those requirements shall take precedence.

Encryption Operation

Outbound email encryption is enforced automatically by the County's email security infrastructure.

Encrypted messages are securely transmitted and made available to recipients through a secure messaging portal or equivalent protected delivery mechanism.

Recipients may be required to authenticate or register with the secure messaging system in order to access encrypted messages.

The specific method of recipient access, including authentication and message retrieval, shall be determined by the County's encryption platform and may evolve over time.

Senders are not required to take action to initiate encryption and will be notified, where applicable, that a message has been secured.

User Responsibilities

Users are responsible for:

- Using County email systems for all official communications;
- Ensuring that information transmitted via email is appropriate, accurate, and necessary;
- Verifying recipient addresses prior to sending messages;
- Avoiding unnecessary transmission of sensitive data where alternative secure methods are available; and
- Reporting any suspected misdirected or improperly transmitted email immediately.

Users shall not attempt to circumvent, disable, or alter encryption controls.

Prohibited Activities

The following activities are prohibited:

- Using personal or unauthorized email accounts to transmit County data;
- Attempting to bypass or disable email encryption controls;
- Transmitting sensitive data through unapproved communication channels;
- Sending information to unauthorized recipients; and
- Any use of email that violates County policy or applicable law.

Incident Reporting

Any suspected or actual unauthorized disclosure of information via email, including misdirected messages or improper transmission of sensitive data, must be reported immediately in accordance with the County's Security Incident and Data Breach Reporting Policy.

Monitoring and Enforcement

Sullivan County reserves the right, subject to applicable law, to monitor email systems and encryption controls to ensure compliance with this policy.

Violations of this policy may result in:

- Restriction or revocation of email access;
- Disciplinary action, up to and including termination; and/or
- Legal action where applicable.

Disclaimer

Sullivan County assumes no liability for damages resulting from unauthorized or improper use of email systems where such use violates this policy, except as otherwise required by law.

SCITS-7020.001 Policy – Copyright and Intellectual Property Compliance

Title	Number
Copyright and Intellectual Property Compliance	**SCITS-7020.001**

Creation Date: **May 2026**

Modified Date:

Purpose

Sullivan County is committed to respecting and protecting the intellectual property rights of others in accordance with applicable federal and state laws.

Advances in technology and electronic communications, including the Internet, cloud services, and digital media platforms, have significantly increased access to copyrighted materials. As a result, the risk of copyright infringement—whether intentional or unintentional—has increased.

The purpose of this policy is to establish standards and expectations to ensure that all County employees and users comply with copyright laws and avoid unauthorized use, reproduction, or distribution of protected materials.

Scope

This policy applies to:

- All Sullivan County employees, elected officials, contractors, consultants, interns, and other authorized users;
- All County-owned or managed systems, devices, and networks; and
- All use of digital or physical materials accessed, stored, transmitted, or reproduced using County resources.

This includes, but is not limited to, use of email, Internet access, file storage systems, cloud services, and software applications.

General Policy

All users of Sullivan County systems are responsible for complying with all applicable copyright laws and licensing requirements.

Sullivan County reserves the right to monitor systems, networks, and stored content to ensure compliance with this policy and applicable law. The County may remove, restrict, or disable access to any materials determined to be in violation of copyright or licensing requirements.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has authority to enforce technical controls and remove unauthorized or infringing materials from County systems. The County Attorney shall provide legal guidance regarding copyright compliance and interpretation.

Permitted Use

Users may access and use copyrighted materials only when:

- The material is in the public domain;
- The use qualifies under applicable legal exceptions (e.g., fair use, where applicable);
- The County holds a valid license or subscription permitting such use; or
- Explicit written permission has been obtained from the copyright holder.

Users must comply with all license agreements, terms of service, and usage restrictions associated with software, digital content, and other materials.

Prohibited Activities

The following activities are strictly prohibited:

- Reproducing, distributing, downloading, uploading, or sharing copyrighted materials without proper authorization or licensing;
- Installing, copying, or using unlicensed or pirated software;
- Using County systems to access or distribute copyrighted media (e.g., music, movies, software, publications) in violation of the law;
- Circumventing digital rights management (DRM) or licensing controls; and
- Storing or transmitting copyrighted materials in violation of licensing agreements or applicable law.

Assumption of Copyright Protection

Users should assume that all materials—whether text, images, audio, video, software, or other content—are protected by copyright unless there is clear evidence that the material is in the public domain or otherwise authorized for use.

Copyright protection does not require registration or the presence of a copyright notice.

Examples of Copyrighted Materials

Copyrighted materials include, but are not limited to:

- Written content (e.g., articles, reports, publications);
- Images, photographs, and graphics;
- Audio recordings and music files;
- Video content and multimedia;
- Software programs and applications; and
- Databases and digital content collections.

Materials not protected by copyright may include:

- Works in the public domain;
- U.S. federal government works (where applicable);
- Facts, ideas, methods, and processes (as distinct from their expression).

Reporting and Guidance

Employees who are uncertain about whether a particular use complies with copyright law or licensing requirements must seek guidance before proceeding.

Questions regarding copyright compliance should be directed to the County Attorney. Technical concerns or removal of materials should be directed to Information Technology Services.

Enforcement

Violations of this policy may result in:

- Removal of unauthorized materials;
- Suspension or restriction of system access;
- Disciplinary action, up to and including termination; and/or
- Legal action where applicable.

Individuals may be held personally responsible for unlawful use of copyrighted materials.

Disclaimer

Sullivan County does not assume liability for unauthorized or unlawful use of copyrighted materials by users in violation of this policy. All users are responsible for ensuring their activities comply with applicable laws and licensing requirements.

SCITS-7030.002 Policy – Use of Artificial Intelligence (AI) in County Operations

Title	Number
Use of Artificial Intelligence (AI) in County Operations	SCITS-7030.002

Creation Date: 12/19/2024 (Resolution # 632-24)

Modified Date: May 2026

Purpose

The purpose of this policy is to establish standards, controls, and governance requirements for the use of Artificial Intelligence (AI) technologies in Sullivan County operations.

Artificial Intelligence is a rapidly evolving class of technologies that can enhance productivity, decision-making, and service delivery. However, AI systems also introduce risks related to data privacy, security, accuracy, bias, legal compliance, and public trust.

Sullivan County recognizes that responsible use of AI can provide operational benefit while inappropriate or uncontrolled use may expose the County to significant legal, regulatory, operational, and reputational risk.

This policy is intended to:

- Ensure AI technologies are used in a secure, ethical, and legally compliant manner;
- Protect County data, including Personal, Private, or Sensitive Information (PPSI), Protected Health Information (PHI), Criminal Justice Information (CJI), and other regulated data;
- Establish clear governance, accountability, and oversight of AI use;
- Define acceptable and prohibited uses of AI; and
- Ensure transparency, human oversight, and responsible decision-making in all AI-assisted processes.

This policy applies broadly to Artificial Intelligence but places particular emphasis on **generative AI technologies**, including but not limited to systems such as Microsoft Copilot, OpenAI ChatGPT, and similar tools.

Scope

This policy applies to:

- All Sullivan County employees, elected officials, contractors, consultants, vendors, interns, and authorized users;
- All County-owned, County-managed, or County-connected systems and data;
- All AI tools, platforms, or services used in connection with County business, whether cloud-based, locally hosted, embedded in vendor systems, or publicly accessible; and
- All environments, including on-premises, cloud, hybrid, and third-party systems.

Use of AI for County business purposes is a privilege and is subject to approval, monitoring, and compliance with this policy and all related County requirements.

Definitions

Artificial Intelligence (AI):
The simulation of human intelligence processes by machines, including systems capable of learning, reasoning, generating content, or making predictions.

Generative AI:
AI systems that generate content such as text, images, code, or other outputs based on user input or prompts.

AI System:
Any application, platform, or service that incorporates artificial intelligence capabilities.

AI Vendor:
Any third-party provider that develops, supplies, or embeds AI functionality within its products or services.

General Policy

Artificial Intelligence shall be used only in a manner that:

- Supports legitimate County business purposes;
- Complies with all applicable laws, regulations, and County policies;
- Protects the confidentiality, integrity, and availability of County data; and
- Maintains public trust through transparency, accountability, and human oversight.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, shall have authority over:

- Approval of AI technologies;
- Oversight of AI usage within County operations;
- Enforcement of AI-related security and governance requirements; and

- Restriction or prohibition of AI tools that present unacceptable risk.

No AI system shall be implemented, integrated, or relied upon for County operations without prior review and approval by Information Technology Services.

AI Risk Classification and Governance

All AI use within Sullivan County shall be evaluated and governed based on risk classification.

AI systems shall be categorized as:

- **Low Risk:** Administrative assistance, drafting, summarization, or general research with no sensitive data involved
- **Moderate Risk:** Internal operational support where outputs influence but do not determine decisions
- **High Risk:** Systems supporting decisions affecting operations, services, or individuals
- **Restricted / Prohibited Risk:** Systems involving regulated data, legal determinations, eligibility decisions, or automated decision-making without human oversight

Use of High Risk AI systems requires:

- Formal review and approval by Information Technology Services;
- Legal and compliance review where applicable; and
- Documented controls ensuring accuracy, accountability, and oversight.

Restricted or Prohibited AI uses shall not be permitted under any circumstances unless explicitly authorized by the CIO in coordination with the County Attorney and Corporate Compliance Office.

Prohibition on Use of Protected or Confidential Data

AI systems shall **not** be used to process, transmit, or generate content containing:

- Personal Identifiable Information (PII);
- Personal, Private, or Sensitive Information (PPSI);
- Protected Health Information (PHI);
- Criminal Justice Information (CJI);
- Financial or payment card data (PCI); or
- Any data protected by federal, state, or local law

unless:

- The AI system has been formally approved by Information Technology Services;
- Appropriate legal agreements (e.g., data protection agreements, BAAs, DPAs) are in place; and
- Technical and administrative safeguards are verified and enforced.

Unauthorized disclosure of protected or confidential data through AI systems may result in disciplinary action, legal consequences, and regulatory reporting obligations.

Ethical and Responsible Use Standards

All AI use must adhere to the following principles:

Equity and Fairness

AI systems must be used in a manner that avoids bias and ensures equitable treatment of all individuals.

Accuracy and Reliability

Users must validate outputs and ensure AI-generated content is accurate, current, and appropriate.

Transparency

Use of AI must be transparent, particularly where outputs are shared externally or influence decisions.

Explainability

AI-assisted decisions must be understandable and explainable by human users.

Privacy and Data Protection

All AI use must comply with applicable privacy laws and County data protection standards.

Human Oversight

AI shall augment—not replace—human decision-making. Final decisions remain the responsibility of authorized County personnel.

Acceptable Uses of AI

Acceptable uses of AI in County operations include:

- Drafting documents, communications, or summaries for internal use;
- Assisting with research or general knowledge inquiries;
- Improving administrative efficiency and workflow;
- Supporting training, simulations, or educational activities;
- Generating non-sensitive test data or development content;
- Assisting with technical troubleshooting; and
- Developing preliminary materials that are reviewed and finalized by a human.

All outputs must be reviewed, validated, and approved prior to use in official County business.

Prohibited Uses of AI

The following uses are strictly prohibited:

- Inputting or exposing protected, confidential, or regulated data into unapproved AI systems;
- Using AI to make final decisions affecting employment, eligibility, legal status, or access to services;
- Publishing AI-generated content without appropriate human review and authorization;
- Generating malicious, deceptive, or unlawful content;
- Using AI in violation of County policy, law, or ethical standards;
- Deploying AI systems that create barriers to access or discriminate against individuals; and
- Implementing AI systems without prior approval from Information Technology Services.

Procurement and Vendor Requirements

All AI systems procured through third-party vendors must:

- Be reviewed and approved by Information Technology Services;
- Meet County security, privacy, and compliance requirements;
- Include contractual safeguards addressing data use, ownership, and protection; and
- Align with County standards for ethical and responsible AI use.

No department may independently procure or implement AI-enabled systems without formal approval.

Training and Awareness

Personnel using AI must:

- Understand the risks, limitations, and appropriate use of AI technologies;
- Complete AI awareness training where required; and
- Remain informed of evolving AI risks and governance expectations.

Transparency and Records Management

Where AI-generated content is used externally or becomes part of a public record:

- The use of AI should be disclosed where appropriate;
- Content must be reviewed and approved by authorized personnel; and
- Records may be subject to retention and disclosure requirements, including FOIL.

Governance and Oversight

No AI system or use case shall be implemented, piloted, or used in production without prior submission and approval through the County's AI review and intake process as defined by Information Technology Services.

All AI use must:

- Align with County policies and applicable laws;
- Be reported to Information Technology Services for awareness and inventory tracking; and
- Be subject to review, monitoring, and restriction as necessary.

Information Technology Services maintains authority to:

- Audit AI usage;
- Restrict or disable AI tools; and
- Enforce compliance with this policy.

Reporting and Incident Response

Any suspected:

- Unauthorized data disclosure;
- Misuse of AI; or
- Security concern related to AI

must be reported immediately to Information Technology Services.

Enforcement

Failure to comply with this policy may result in:

- Suspension or revocation of system access;
- Disciplinary action;
- Termination of employment or contract; and/or
- Legal or regulatory action.

Assistance

For questions regarding AI use, implementation, or compliance, contact the Information Technology Services Help Desk.

Section 8 — Third-Party, Vendor, and External Asset Control (8000 Series)

SCITS-8000.001 Policy – Third-Party Access and Vendor Security

Title	Number
Third-Party Access and Vendor Security	**SCITS-8000.001**

Creation Date: **May 2026**

Modified Date:

Purpose

Third-party access to Sullivan County systems, facilities, and data introduces significant operational, cybersecurity, legal, and reputational risk. Such access must be carefully controlled, monitored, and governed to ensure the protection of County information and technology resources.

The purpose of this policy is to establish requirements governing third-party access to County systems, networks, facilities, and data, and to define the responsibilities of both third parties and County personnel in managing such access.

Scope

This policy applies to:

- All third parties, including but not limited to vendors, contractors, consultants, service providers, business partners, and external support personnel;
- All County systems, networks, applications, and data;
- All physical access to County information technology facilities, including data centers and equipment rooms; and
- All County personnel responsible for engaging, managing, or supervising third parties.

Third-party access is a privilege, not a right, and shall be granted only where a valid business need exists and appropriate controls are in place.

General Policy

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has authority over the approval, control, monitoring, and termination of all third-party access to County systems, networks, and information technology facilities.

All third-party access must be:

- Authorized in advance;
- Limited to the minimum necessary to perform contracted work (least privilege);
- Time-bound and subject to periodic review; and
- Governed by appropriate contractual, legal, and security requirements.

No third party shall be granted access to County systems or facilities without appropriate authorization, documentation, and oversight.

Physical Access to Information Technology Facilities

Access to County data centers, server rooms, and other secured technology areas shall be strictly controlled.

The following requirements apply:

- All third-party physical access must be scheduled in advance and approved by Information Technology Services;
- Access shall occur during normal business hours unless otherwise authorized;
- Third parties must be escorted at all times by authorized County personnel;
- A designated Information Technology representative shall supervise or coordinate all work performed;
- Third parties must clearly describe the scope and purpose of work prior to beginning any activity;
- Information Technology Services shall define and enforce all required safeguards to protect systems, equipment, and data; and
- Access shall be revoked immediately upon completion of work or termination of the engagement.

All third-party physical access shall be logged and documented.

System and Network Access

Third-party access to County systems and networks must comply with the following:

- Access must be uniquely assigned to an identifiable individual and must not be shared;
- Authentication and credential management must comply with County Identity and Access Management and Password policies;

- Access must be provisioned using secure methods approved by Information Technology Services;
- Remote access must utilize County-approved secure access mechanisms (e.g., VPN, MFA-protected access);
- Access must be restricted to only those systems, applications, and data required to perform authorized work; and
- Access shall be disabled immediately upon completion of work or termination of the engagement.

Information Technology Services shall determine and enforce appropriate network security controls, including segmentation, monitoring, and logging.

Contractual and Security Requirements

All third-party engagements involving access to County systems or data must include appropriate contractual provisions, which may include, but are not limited to:

- Defined scope of work, access requirements, and authorized work hours;
- Data access limitations and handling requirements;
- Compliance with all applicable laws, regulations, and County policies;
- Execution of non-disclosure or confidentiality agreements;
- Security requirements, including system hardening, patching, and malware protection;
- Requirements for secure remote access;
- Requirements for incident reporting and cooperation in investigations;
- Requirements for return or destruction of County data at the conclusion of the engagement; and
- Requirements for return of County-owned equipment and assets.

All contracts shall be reviewed and approved in accordance with County procurement, legal, and information technology requirements.

Data Protection and Confidentiality

Third parties shall:

- Access only the data necessary to perform authorized work;
- Protect all County data from unauthorized access, disclosure, alteration, or destruction;
- Not use County data for any purpose other than fulfilling contractual obligations;
- Not disclose County data to any unauthorized party; and
- Comply with all applicable data protection and privacy laws and regulations.

All sensitive or regulated data must be handled in accordance with County policies and applicable legal requirements.

Third-Party Security Requirements

Third parties must meet minimum security standards as defined by Information Technology Services, which may include:

- Use of up-to-date endpoint protection and system patching;
- Secure configuration of systems used to access County resources;
- Compliance with County-approved access methods and controls;
- Participation in security reviews or assessments where required; and
- Adherence to County change management and operational procedures.

Third-party systems or devices that do not meet required security standards shall not be permitted to connect to County systems.

Subcontractors and Personnel

Third parties must:

- Provide a current list of all personnel and any subcontractors requiring access;
- Ensure that all personnel are authorized and qualified to perform assigned work;
- Notify the County promptly of any personnel changes affecting access; and
- Ensure that all individuals comply with County policies and contractual requirements.

Third-party personnel must be identifiable and accountable for all actions performed.

Monitoring, Auditing, and Oversight

Sullivan County reserves the right, subject to applicable law, to monitor, log, and audit third-party access and activity to ensure compliance with this policy and contractual requirements.

Third parties must cooperate with audits, reviews, and investigations conducted by or on behalf of the County.

Documentation of third-party activities, including access logs, changes, and deliverables, shall be maintained and made available upon request.

Incident Reporting and Response

Third parties must immediately report any actual or suspected security incident, data breach, or unauthorized access involving County systems or data.

Where third parties are involved in incident response activities, roles and responsibilities shall be defined in contractual agreements.

Third parties must fully cooperate with County-led incident response and remediation efforts.

Termination of Access and Data Handling

Upon completion or termination of a third-party engagement:

- All access to County systems and facilities shall be immediately revoked;
- All County data must be returned or securely destroyed as directed by the County;
- Written certification of data destruction must be provided where applicable;
- All County-owned equipment, credentials, access devices, and identification must be returned; and
- Any retained materials must be explicitly authorized and documented.

Timeframes for data return or destruction shall be defined in contractual agreements or as directed by the County.

Enforcement

Failure to comply with this policy may result in:

- Immediate suspension or termination of access;
- Termination of contractual agreements;
- Financial or legal remedies; and/or
- Other actions as deemed appropriate by Sullivan County.

Disclaimer

Sullivan County assumes no liability for damages resulting from third-party failure to comply with this policy or applicable contractual obligations, except as otherwise required by law.

SCITS-8010.001 – Technology Services Procurement Policy

Title	Number
Technology Services Procurement Policy	**SCITS-8010.001**

Creation Date: **May 2026**

Modified Date:

Purpose

The purpose of this policy is to establish standardized requirements, governance controls, and approval procedures for the procurement, leasing, subscription, renewal, or use of all technology-related services utilized by Sullivan County.

Technology services include, but are not limited to, cloud-based platforms, Software-as-a-Service (SaaS) solutions, hosted systems, managed services, third-party integrations, and consulting or professional services that interact with, support, or impact County systems or data.

This policy is intended to:

- Ensure that all technology services align with County cybersecurity, architectural, operational, and compliance requirements;
- Protect County systems and data from risks associated with third-party services and external access;
- Promote consistent, secure, and cost-effective use of technology services; and
- Maintain centralized oversight, accountability, and control over all technology service relationships.

Scope

This policy applies to:

- All Sullivan County departments, offices, agencies, and units;
- All employees, elected officials, contractors, consultants, vendors, and authorized users; and
- All technology service acquisitions regardless of funding source, including operating budgets, capital funds, grants, reimbursements, or purchasing cards.

This policy applies to all technology-related services, including but not limited to:

- Cloud storage, hosting, and infrastructure services;
- Software-as-a-Service (SaaS) platforms and subscription services;
- External application hosting or data processing services;
- Managed IT or security services;
- Third-party integrations or API-connected systems;
- Vendor-supported systems or externally administered platforms; and
- External consultants or service providers with access to County systems, networks, or data.

General Policy

All technology services shall be subject to the review, approval, and control of the Department of Information Technology Services (ITS) under the authority of the Commissioner of Information Technology / Chief Information Officer (CIO).

No County department, office, or unit shall independently procure, lease, subscribe to, renew, implement, or utilize any technology service without prior review and written approval by ITS.

All technology service engagements must comply with County procurement procedures and shall be evaluated for security, compatibility, supportability, and compliance prior to approval.

In accordance with County governance and **Resolution No. 110-24**, any software or system provided through a technology service, including SaaS platforms, shall be under the control and jurisdiction of Information Technology Services and subject to centralized oversight, management, and inventory.

Approval Requirements

All technology service requests must:

- Be submitted through the County's established procurement and IT request processes;
- Include sufficient documentation describing the business need, scope of service, data involved, and funding source; and
- Receive formal review and written approval from Information Technology Services prior to execution of any agreement or engagement.

Purchasing, Finance, or any other approving authority shall not process any purchase order, contract, agreement, or payment for technology services without documented ITS approval.

No department shall enter into any agreement, contract, memorandum of understanding, or informal arrangement with a technology service provider without such approval.

Technology, Security, and Risk Review

No service shall be approved where the County cannot ensure administrative control, audit capability, and timely retrieval of its data. Information Technology Services shall evaluate all proposed technology services for:

- Cybersecurity risks, including external access, data exposure, and system integration;
- Compliance with applicable laws, regulations, and standards (e.g., HIPAA, CJIS, PCI-DSS, FOIL, records retention);
- Data ownership, storage location, and jurisdiction;
- Vendor security practices, controls, and breach notification obligations;
- Integration with County systems and infrastructure;
- Identity and access management requirements;
- Backup, recovery, and business continuity capabilities; and
- Operational support, lifecycle management, and vendor dependency risk.

ITS may approve, conditionally approve, or deny any proposed service based on these factors.

Third-Party Access and Control

No external vendor, consultant, or service provider shall be granted access to County systems, networks, or data without:

- Prior approval by Information Technology Services;
- Appropriate contractual protections, including confidentiality, security, and data protection requirements; and
- Implementation of County-approved access controls and monitoring.

All third-party access shall be:

- Limited to the minimum necessary to perform authorized services;
- Time-bound and subject to periodic review; and
- Revoked promptly when no longer required.

Contracting, Licensing, and Ownership

All agreements for technology services:

- Shall be executed in the name of the County of Sullivan;
- Shall clearly define data ownership, with all County data remaining the property of Sullivan County;
- Shall include provisions for data access, export, retention, and return upon termination; and
- Shall be subject to review by Information Technology Services for technical, security, and operational requirements.

Departments shall not accept “free,” trial, pilot, grant-funded, or vendor-provided services without ITS review and approval.

Implementation and Integration

All approved technology services shall be:

- Implemented and integrated under the direction of Information Technology Services;
- Configured to comply with County security, monitoring, and access control standards; and
- Managed in coordination with County systems, identity platforms, and operational processes.

Unauthorized use of external services or “shadow IT” solutions is strictly prohibited.

Exceptions

Any exception to this policy must:

- Be formally requested in writing;
- Include a documented business justification and risk acknowledgment; and
- Receive explicit written approval from the CIO or designee.

Approved exceptions may be subject to compensating controls, restrictions, or periodic review.

Enforcement

Failure to comply with this policy may result in:

- Denial or cancellation of procurement requests;
- Termination or suspension of unauthorized services;
- Removal of vendor or consultant access;
- Revocation of access to County systems;
- Administrative or disciplinary action; and/or
- Financial responsibility for unauthorized engagements, where applicable.

Technology services acquired or used outside of this policy shall not be supported, secured, or connected to County systems.

Authority and References

This policy is adopted pursuant to Sullivan County governance authority and applicable information technology oversight responsibilities.

In accordance with Resolution No. 110-24, all software and systems utilized by any Division, Department, Office, Agency, or Unit of the County, including those delivered through technology

services, shall be under the control and jurisdiction of the Department of Information Technology Services and subject to centralized management, oversight, and inventory.

All technology service engagements must comply with this requirement.

Disclaimer

Sullivan County assumes no responsibility for technology services procured, implemented, or used without proper authorization. Unauthorized services may be suspended, disconnected, or terminated without notice to protect County systems, data, and operations.

SCITS-8020.001 Technology Equipment and Software Acquisition Policy

Title	Number
Technology Equipment and Software Acquisition Policy	**SCITS-8020.001**

Creation Date: **May 2026**

Modified Date:

Purpose

The purpose of this policy is to establish standardized requirements, governance controls, and approval procedures for the acquisition, licensing, leasing, subscription, or renewal of all technology equipment, software, and related services used by Sullivan County.

This policy is intended to:

- Ensure that all technology acquisitions align with County cybersecurity, architecture, operational, and compliance requirements;
- Reduce risk associated with unauthorized, unsupported, or insecure technologies;
- Promote cost-effective, standardized, and supportable solutions; and
- Maintain centralized accountability, inventory, licensing, and lifecycle management of County technology assets.

Scope

This policy applies to:

- All Sullivan County departments, offices, agencies, and units;
- All employees, elected officials, contractors, consultants, and authorized users; and
- All technology acquisitions regardless of funding source, including operating budgets, capital funds, grants, reimbursements, or purchasing cards.

This policy applies to all technology assets, including but not limited to:

Technology Equipment

Any hardware device that connects to, supports, or stores data for County systems, including but not limited to:

- Desktop computers, laptops, and tablets;
- Servers and infrastructure equipment;
- Printers, scanners, and multifunction devices;
- Mobile devices and peripherals;
- Storage devices, including USB drives and external media;
- Cameras, IoT devices, and specialized equipment; and
- Networking or communication devices.

Software and Technology Services

Any software, system, platform, or service used to process, store, transmit, or access County data, including:

- Installed applications and operating systems;
- Cloud-based or Software-as-a-Service (SaaS) platforms;
- Databases and data processing systems;
- Web-based tools, plugins, or extensions;
- Subscription services and hosted solutions; and
- Any system that integrates with or connects to County systems or data.

General Policy

All technology equipment and software acquisitions shall be subject to the review, approval, and control of the Department of Information Technology Services (ITS) under the authority of the Commissioner of Information Technology / Chief Information Officer (CIO).

No County department, office, or unit shall independently purchase, lease, subscribe to, renew, install, or otherwise acquire any technology equipment or software without prior review and approval by ITS.

All technology acquisitions must follow County procurement procedures and shall be evaluated for security, compatibility, supportability, and compliance prior to approval.

Approval Requirements

All technology-related purchases and acquisitions must:

- Be submitted through the County's established procurement and IT request processes;
- Include sufficient documentation describing the business need, intended use, and funding source; and
- Receive formal review and approval from Information Technology Services prior to procurement.

Purchasing, Finance, or any other approving authority shall not process any purchase order, contract, or payment for technology equipment or software without documented ITS approval.

ITS approval shall confirm that the proposed acquisition:

- Meets County cybersecurity and data protection requirements;
- Is compatible with existing systems, architecture, and standards;
- Can be supported, maintained, and secured by the County;
- Does not introduce unacceptable risk; and
- Aligns with County technology strategy and operational needs.

Technology and Security Review

Information Technology Services shall evaluate all proposed acquisitions for:

- Cybersecurity risks, including data exposure, access control, and external connectivity;
- Compliance with applicable laws, regulations, and standards (e.g., HIPAA, CJIS, PCI-DSS, FOIL, records retention);
- Integration with existing systems and infrastructure;
- Vendor security practices and contractual protections;
- Data ownership, storage location, and recovery capabilities; and
- Lifecycle considerations, including support, patching, and end-of-life risk.

ITS may approve, conditionally approve, or deny any acquisition based on these factors.

Contracting, Licensing, and Ownership

All software, licenses, subscriptions, and related agreements:

- Shall be issued in the name of the County of Sullivan;
- Shall be centrally managed, tracked, and maintained by Information Technology Services; and
- Shall not be procured, accepted, or renewed independently by departments.

Departments shall not accept “free,” trial, pilot, grant-funded, or vendor-provided software or services without ITS review and approval.

Inventory and Asset Management

All technology equipment and software acquired by or on behalf of the County shall be:

- Recorded and maintained in the County’s official asset inventory system;
- Tracked for lifecycle management, support, licensing, and audit purposes; and
- Reported as required to appropriate County oversight functions.

Departments shall cooperate with Information Technology Services to ensure accurate inventory and accountability.

Implementation and Deployment

All approved technology shall be:

- Installed, configured, and deployed by Information Technology Services or under its direction;
- Integrated into County security, monitoring, backup, and support frameworks; and
- Managed in accordance with County standards and operational procedures.

Unauthorized installation or use of unapproved hardware or software is strictly prohibited.

Exceptions

Any exception to this policy must:

- Be formally requested in writing;
- Include a documented business justification and risk acknowledgment; and
- Receive explicit written approval from the CIO or designee.

Approved exceptions may be subject to compensating controls, limitations, or periodic review.

Enforcement

Failure to comply with this policy may result in:

- Denial or cancellation of procurement requests;
- Removal or disabling of unauthorized technology;
- Revocation of access to County systems;
- Administrative or disciplinary action; and/or
- Financial responsibility for unauthorized purchases, where applicable.

Technology acquisitions made outside of this policy shall not be supported, secured, or connected to County systems.

Authority and References

This policy is adopted pursuant to Sullivan County governance authority and applicable information technology oversight responsibilities.

In accordance with Resolution No. 110-24, all software utilized by any Division, Department, Office, Agency, or Unit of the County shall be under the control and jurisdiction of the Department of

Information Technology Services, shall be licensed to the County of Sullivan, and shall be subject to centralized management, inventory, and oversight by Information Technology Services.

All technology acquisitions and implementations must comply with this requirement.

Disclaimer

Sullivan County assumes no responsibility for technology equipment or software acquired, installed, or used without proper authorization. Unauthorized solutions may be removed, disabled, or denied access without notice to protect County systems, data, and operations.

SCITS-8030.001 Policy – Domain Name System (DNS) and Domain Registration Policy

Title	Number
Domain Name System (DNS) and Domain Registration Policy	**SCITS-8030.001**

Creation Date: **May 2026**

Modified Date:

Purpose

To establish centralized control over the registration, ownership, and management of internet domain names used to support Sullivan County operations, services, and public communications.

Domain names are County-owned digital assets tied directly to security, legal ownership, and public trust, and must be centrally controlled by Information Technology Services (ITS) to prevent loss, misuse, or service disruption.

Scope

This policy applies to:

- All Sullivan County departments, agencies, boards, and affiliated entities;
- All internet domain names representing or associated with Sullivan County; and
- All domain registration, renewal, transfer, and DNS management activities.

General Policy

Domain names are considered County information assets and are subject to all applicable County security, access control, and asset management policies.

All domain registrations conducted on behalf of Sullivan County or any County agency shall be performed exclusively through Information Technology Services (ITS).

No department, employee, contractor, or third party is authorized to independently register, renew, transfer, or manage domain names representing County business without the prior approval and involvement of ITS.

All domains shall be registered in a manner that ensures Sullivan County retains sole ownership, administrative control, and recovery authority at all times.

Ownership and Control

- All domain names shall be registered using County-controlled accounts and contact information.
- Administrative, technical, and billing contacts shall be maintained by ITS.
- Domains shall not be registered using personal email addresses, personal accounts, or third-party-owned credentials.
- ITS shall maintain an authoritative inventory of all County domains.

DNS and Configuration Management

- DNS configuration, hosting, and changes shall be managed or approved by ITS.
- Security controls, including registrar protections (e.g., domain lock, multi-factor authentication, and access restrictions), shall be implemented where supported.
- Unauthorized changes to DNS records are prohibited.

Renewal and Lifecycle Management

- ITS shall be responsible for domain renewal tracking and execution.
- Departments shall not independently renew domains.
- Domains no longer required shall be formally decommissioned in coordination with ITS.

Third-Party and Vendor Use

- Any vendor requiring domain access must do so under ITS oversight.
- Domains shall not be registered or held in vendor-owned accounts on behalf of the County.
- Contractual agreements must reflect County ownership and control of all domains.

Monitoring and Enforcement

Sullivan County reserves the right, subject to applicable law, to monitor, audit, and review domain registrations and DNS configurations to ensure compliance with this policy.

Failure to comply with this policy may result in:

- Revocation of access;
- Removal or transfer of domain control;
- Disciplinary or contractual action; and/or
- Other actions as deemed appropriate by Sullivan County.

Exception Process

Exceptions to this policy must be formally requested and approved in writing by the Commissioner of Information Technology / Chief Information Officer (CIO).

Section 9 — Incident Response and Security Operations (9000 Series)

SCITS-9000.001 Policy – Incident Response and Cybersecurity Event Management

Title	Number
Incident Response and Cybersecurity Event Management	**SCITS-9010.001**
Creation Date: **March 2025**	
Modified Date: **May 2026**	

Purpose

The purpose of this policy is to establish a standardized, county-wide framework for identifying, reporting, assessing, responding to, and recovering from cybersecurity incidents and information security events.

Sullivan County recognizes that cybersecurity incidents—including, but not limited to, ransomware, data breaches, system compromise, unauthorized access, and service disruption—pose significant operational, legal, financial, and reputational risk.

This policy is intended to:

- Ensure timely and coordinated response to incidents;
- Minimize impact to County operations, systems, and data;
- Support legal, regulatory, and contractual compliance obligations;
- Preserve evidence for investigation and potential legal action; and
- Restore services in a controlled and secure manner.

Scope

This policy applies to:

- All Sullivan County employees, elected officials, contractors, vendors, and authorized users;
- All County-owned, County-managed, or County-connected systems, networks, devices, and data;
- All third-party systems or services that store, process, or transmit County information; and
- All environments, including on-premises, cloud, mobile, remote access, and hybrid systems.

This policy applies to all suspected or confirmed cybersecurity incidents, regardless of severity.

Definitions

Security Event: Any observable occurrence that may indicate a potential security issue.

Incident: A confirmed or reasonably suspected event that threatens confidentiality, integrity, or availability.

Breach: An incident involving unauthorized acquisition or exposure of protected or regulated data.

Information Technology Services (ITS) shall determine when a security event meets the threshold of a reportable incident.

Containment: Actions taken to limit spread or impact.

Eradication: Removal of the root cause.

Recovery: Restoration of systems and services.

General Policy

All cybersecurity incidents shall be:

- Reported immediately;
- Assessed promptly;
- Escalated appropriately;
- Managed under centralized authority; and
- Documented and reviewed.

The County adopts a risk-based, coordinated incident response approach aligned with **NIST SP 800-61**.

Detailed incident response procedures, communication protocols, and operational runbooks maintained by Information Technology Services (ITS) support and operationalize this policy. These documents are controlled separately and may be updated as required to address evolving threats, technologies, and operational needs.

Incident Response Authority

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, shall have final operational authority over all cybersecurity incident response activities.

The CIO is authorized to:

- Direct and coordinate incident response actions;
- Isolate or disconnect systems;
- Disable accounts or access;
- Engage third-party cybersecurity or forensic services;
- Require immediate remediation actions;
- Preserve or restrict access to systems and data; and

- Escalate to executive leadership, legal counsel, or law enforcement.

The CIO is authorized to take immediate protective action without prior approval where delay would increase risk to County systems, operations, or data. Actions taken under this policy that impact personnel shall be carried out in coordination with applicable personnel policies, collective bargaining agreements, and legal requirements.

All departments shall comply with incident response directives issued by the CIO.

Executive Oversight and Decision Authority

The County Manager shall serve as the executive authority responsible for strategic, operational, and risk-based decisions during significant cybersecurity incidents.

While the Commissioner of Information Technology / Chief Information Officer (CIO) retains full operational command of incident response activities, the County Manager shall be engaged for incidents classified as **High or Critical** to:

- Approve or acknowledge major operational decisions impacting County-wide services;
- Authorize significant business continuity measures or service prioritization;
- Provide executive direction regarding risk acceptance where immediate restoration actions may limit forensic preservation;
- Coordinate with elected officials and senior leadership; and
- Support external coordination at the executive or intergovernmental level, as appropriate.

Decisions regarding ransom engagement, including negotiation or non-payment, shall be made in coordination with the County Manager, County Attorney, and law enforcement, as appropriate.

Nothing in this section shall be construed to delay immediate response actions directed by the CIO where time-sensitive containment or protection of County systems is required.

Incident Reporting Requirements

All users must report suspected or confirmed incidents immediately, and no later than one (1) hour from discovery, except where operationally infeasible, in which case reporting must occur as soon as possible. Suspected or confirmed incidents include:

- Phishing or suspicious emails;
- Malware or ransomware activity;
- Unauthorized access alerts;
- Lost or stolen devices;
- Data exposure or misdirected communications; and
- System anomalies or unusual behavior.

Reports shall be made to:

- Information Technology Services (Help Desk or security channel); and/or

- Supervisor or Department Head.

Failure to report may result in disciplinary action.

Incident Notification and Escalation Protocol

Sullivan County maintains a defined escalation protocol to ensure rapid engagement of appropriate resources.

For **High or Critical incidents**, including ransomware, widespread compromise, or potential exposure of regulated data:

1. **New York State Division of Homeland Security and Emergency Services (NYS DHSES) Cyber Incident Response Team** shall be notified immediately.
2. **Information Technology Services (ITS)** shall continue coordinated response under CIO authority.
3. **Corporate Compliance Office** shall be notified where regulated data may be involved.
4. **County Attorney** shall be notified for legal and regulatory guidance.
5. **County Manager** shall be notified as soon as practicable following initial stabilization and State notification.

For lower-severity incidents, notification may follow standard internal escalation procedures as determined by ITS.

The CIO retains authority to modify notification sequencing based on incident conditions.

All notifications shall be documented.

Nothing in this section shall be construed to delay notification to State or Federal authorities where immediate reporting is required or appropriate.

Incident Response Team (IRT) Structure

Sullivan County maintains a defined Incident Response Team (IRT) operating under centralized command.

Incident Commander (CIO)

- Full operational authority
- Directs all response actions
- Balances recovery versus forensic preservation

Operations Lead (ITS)

- Executes technical response
- Coordinates IT staff, administrators, and vendors

Legal and Compliance Liaison

- Corporate Compliance Office and County Attorney
- Determines breach obligations and regulatory requirements

State / External Liaison

- Coordinates with NYS DHSES and other external partners

Communications Lead

- Controls internal and external messaging

Business / Department Liaison

- Communicates operational impacts and priorities

Security / Forensics Lead

- Conducts technical analysis and investigation

Documentation Lead

- Maintains timeline, decisions, records, and notifications

Law Enforcement Liaison (as required)

- District Attorney's Office and/or appropriate internal/external agencies
- Engaged at the direction of the Incident Commander in consultation with the County Attorney
- Coordinates criminal investigation where applicable

No individual outside of the Incident Response Team (IRT), or without explicit authorization from the Incident Commander, may direct response actions or communicate externally on behalf of the County during an incident.

Incident Classification

Low
Minimal impact.

Moderate
Limited disruption.

High
Significant operational or data impact. Examples:

- Single system compromise with elevated privileges
- Disruption of critical business systems
- Active malware with lateral movement potential

Critical
Confirmed breach, ransomware, or widespread compromise. Examples:

- Ransomware execution or encryption activity
- Confirmed or suspected exfiltration of regulated data
- Multi-system or domain-wide compromise

Classification shall determine escalation, response priority, and notification requirements.

Incident Response Process

1. Identification
    - Detect and validate event;
    - Determine scope and impact;
    - Initiate documentation and tracking.
2. Containment
    - Isolate systems;
    - Prevent spread;
    - Stabilize affected environments.
3. Eradication
    - Remove root cause;
    - Apply fixes, patches, and security controls.
4. Recovery
    - Restore systems and services;
    - Validate system integrity;
    - Monitor for recurrence.
5. Post-Incident Review
    - Conduct after-action review;
    - Identify control gaps and lessons learned;
    - Implement improvements.

Response actions shall be proportional to the risk presented and implemented in a manner that supports operational continuity while maintaining compliance with applicable governance and legal requirements.

Evidence Preservation

Evidence collected during an incident shall be handled in accordance with documented chain-of-custody procedures, including identification, collection, transfer, analysis, and storage, to preserve its integrity and admissibility for investigative, legal, or regulatory purposes, to the extent practicable and consistent with operational priorities, including the restoration of critical County services. Documentation shall include the justification for any deviation from standard evidence preservation procedures, the systems affected, actions taken, and the potential impact on forensic analysis.

All incidents shall be handled to preserve evidence for:

- Forensic investigation;
- Legal proceedings; and
- Regulatory review.

Users shall not:

- Delete files;

- Power off systems, unless directed; or
- Attempt self-remediation.

Business Continuity and Evidence Preservation Exception:

In the event of a cybersecurity incident, Sullivan County will make reasonable efforts to preserve evidence. However, where essential government services, public safety operations, or regulated clinical services are impacted, restoration and continuity may take precedence.

The CIO, in coordination with Corporate Compliance and the County Attorney where practicable, is authorized to proceed with restoration prior to full evidence preservation. All such decisions shall be documented, including the rationale, affected scope, and any limitations placed on subsequent forensic analysis.

Where evidence preservation is limited due to operational necessity, the County shall take reasonable compensating measures, including but not limited to log preservation, system imaging where feasible, and engagement of qualified incident response or forensic resources.

Priority shall be given to restoration of systems supporting life safety, emergency response, public health operations, financial operations essential to continuity, and other mission-critical services as defined by the County.

Legal, Compliance, and Notification Requirements

Where regulated data is involved, the County shall comply with:

- New York State Information Security Breach and Notification Act;
- HIPAA / HITECH;
- 42 CFR Part 2;
- CJIS Security Policy;
- PCI DSS; and
- Article 28 / NYSDOH requirements.

The **Corporate Compliance Office** is the primary intake for breach matters.

The **County Attorney** shall:

- Provide legal guidance;
- Determine notification obligations; and
- Coordinate disclosures.

Where incident response activities involve personnel actions or investigations, such activities shall be conducted in coordination with appropriate administrative and legal authorities.

No external notification shall occur without coordination with Corporate Compliance, the County Attorney, and the CIO, except where immediate reporting is required by law or authorized under this plan.

Third-Party Incident Management

Third parties must:

- Report incidents immediately, and no later than twenty-four (24) hours from discovery, or sooner where required by contract or law;
- Cooperate fully with County investigation and response efforts; and
- Comply with contractual obligations, including security and breach notification requirements.

The County may:

- Require forensic investigation;
- Audit response actions; and
- Suspend or terminate access.

Communication and Coordination

All communications shall be:

- Controlled;
- Authorized; and
- Documented.

Public communications shall be managed through County leadership, the County Attorney, and designated communications personnel, as appropriate.

Training and Preparedness

The County shall:

- Conduct incident response training and awareness;
- Perform exercises and tabletop simulations, where appropriate; and
- Ensure role readiness among key personnel.

Enforcement

Failure to comply with this policy may result in:

- Revocation of access;
- Disciplinary action;
- Termination of employment or contract; and/or
- Legal or regulatory consequences.

Actions taken under this policy that impact personnel shall be carried out in coordination with applicable personnel policies, collective bargaining agreements, and legal requirements.

Final Operational Statement

This policy constitutes the County's authoritative framework for cybersecurity incident response and is designed to support rapid operational decision-making, executive oversight, legal and regulatory compliance, continuity of essential public services, and defensible documentation of County actions during and after significant cyber events.

Document History

March 20, 2025	*IRP creation and publication.*
February 24, 2026	*Annual review with additions covering Corporate Compliance inclusion and specific citation of State and Federal regulations*

SCITS-9005.001 Policy – Incident Response Standard Operating Procedure (SOP)

Title	Number
Incident Response Standard Operating Procedure (SOP)	**SCITS-9005.001**

Creation Date: **March 2025**

Modified Date: **May 2026**

Purpose

This Standard Operating Procedure (SOP) defines the operational steps and coordination processes used by Information Technology Services (ITS) to respond to cybersecurity incidents and significant IT service disruptions.

This SOP operationalizes the County's Incident Response Policy and aligns with NIST SP 800-61. All actions taken under this SOP are performed under the authority established in ITS2026-014 – Incident Response and Cybersecurity Event Management Policy.

Scope

This SOP applies to:

- All ITS personnel
- All County systems, applications, and infrastructure
- All incidents classified under the County Incident Response Policy

Operational Principles

All incident response activities shall adhere to the following:

- Centralized command under the **Incident Commander (CIO or designee)**
- Controlled and authorized communication
- Real-time documentation of all actions and decisions
- Rapid mobilization and coordinated response
- Alignment with legal, regulatory, and operational priorities

Incident Intake and Initial Assessment

Trigger Events

An incident may be identified through:

- Help desk calls
- Monitoring systems or alerts
- User reports
- Vendor notifications
- Direct observation by ITS staff

Initial Actions (Immediate)

1. **Open an incident record/ticket**
2. **Document initial details:**
    - Time detected
    - Reporting source
    - Systems or services affected
3. **Perform initial triage:**
    - Determine if this is:
        - Security-related
        - Operational/system failure
4. **Assign preliminary severity classification**
5. **Escalate to Incident Commander if:**
    - The incident is classified as High or Critical; or
    - The scope, impact, or nature of the incident is uncertain but has the potential to escalate.

Incident Notification and Mobilization

Role-Based Escalation (No Named Individuals)

Notify, as appropriate:

- Incident Commander (CIO or designee)
- Operations Lead
- Security / Forensics Lead
- Additional technical staff based on incident type

Incident Bridge Activation (High / Critical Incidents)

For High or Critical incidents:

- A **dedicated incident bridge** (conference line or virtual meeting) shall be established within **5 minutes**
- All assigned personnel shall:
    - Join immediately
    - Remain available for the duration of the incident

- If the bridge disconnects, it must be **re-established immediately**

Scribe Assignment

- A **Documentation Lead (scribe)** shall be assigned
- Responsible for:
  - Capturing timeline of events
  - Recording decisions and actions
  - Tracking communications

Communication Control

- All communications must be:
  - Authorized
  - Coordinated
  - Documented
- No external communication (including vendors, public, regulatory bodies, or law enforcement) shall occur without explicit authorization from the Incident Commander or designated authority.
- Communication to impacted departments shall be:
  - Coordinated through the Incident Commander or Communications Lead
  - Prioritized based on operational impact

Incident Response Execution (NIST-Aligned)

Phase 1 – Identification

- Validate incident
- Determine scope and impact
- Begin documentation

Phase 2 – Containment

- Isolate affected systems
- Disable compromised accounts
- Prevent lateral spread
- Stabilize environment

Phase 3 – Investigation & Analysis

- Gather logs and system data
- Identify:
  - Root cause
  - Scope of compromise
  - Potential data exposure

- Engage external resources if required

Phase 4 – Eradication

- Remove malicious artifacts
- Eliminate vulnerabilities
- Apply patches and controls
- Reset credentials as needed

Phase 5 – Recovery

- Restore systems from clean state
- Validate integrity before reconnecting
- Monitor for recurrence

Phase 6 – Post-Incident Review

- Conduct after-action review
- Identify gaps and improvements
- Document lessons learned

Special Operational Considerations

Public Safety and Critical Services

Where incidents impact:

- Public safety systems
- Emergency response
- Health or clinical operations

ITS shall:

- Prioritize rapid situational awareness
- Coordinate directly with affected entities
- Escalate immediately to Incident Commander

Vendor Engagement

- Vendors may be engaged as needed
- Must operate under ITS direction
- May be required to join incident bridge

Documentation Requirements

The Documentation Lead shall ensure:

- All actions are logged in real time

- All personnel involved are recorded
- All decisions are documented, including:
  - Rationale
  - Alternatives considered
- All communications are tracked

Operational Rules

- All response actions are directed by the Incident Commander
- No unauthorized deviation from established command structure
- No independent remediation actions without coordination
- All activities must be documented

Maintenance

This SOP shall be:

- Reviewed annually
- Updated as needed to reflect:
  - Technology changes
  - Threat landscape evolution
  - Organizational structure updates

Document History

March 13, 2025	*IRSOP creation and publication.*
March 25, 2026	*Annual review with additions aligning with NIST standards.*

SCITS-9010.001 Policy – Security Incident and Data Breach Reporting

Title	Number
Security Incident and Data Breach Reporting	SCITS-9010.001

Creation Date: May 2026

Modified Date:

Purpose

The purpose of this policy is to establish requirements for the prompt identification, reporting, escalation, and management of suspected or confirmed security incidents and data breaches involving Sullivan County systems or information.

This policy is intended to protect the confidentiality, integrity, and availability of County data, including "personal or private information" as defined under applicable New York State law, and to ensure timely compliance with all legal, regulatory, and operational obligations.

Scope

This policy applies to:

- All Sullivan County employees, elected officials, contractors, consultants, vendors, interns, and other authorized users;
- All County systems, networks, applications, and data;
- All incidents involving suspected or confirmed unauthorized access, acquisition, disclosure, alteration, or destruction of County data; and
- All data classified as confidential, sensitive, or regulated, including personal or private information.

For purposes of this policy, a **data breach** or **compromise of personal or private information** includes the unauthorized acquisition or access of electronic data containing such information.

Encrypted data shall be considered compromised if the encryption key or method necessary to render the data readable is also accessed or acquired.

General Policy

All users have an affirmative obligation to immediately report any known or suspected security incident or data breach.

Failure to report a suspected incident may result in increased risk to County operations, legal exposure, and regulatory non-compliance.

The Commissioner of Information Technology / Chief Information Officer (CIO), in coordination with Corporate Compliance and the County Attorney, has authority over the technical investigation, containment, and response to security incidents.

The Corporate Compliance Office shall serve as the primary intake and coordination point for suspected data breaches involving personal or private information, except where immediate technical response by Information Technology Services is required to contain an active threat.

Reporting Requirements

Any user who becomes aware of or reasonably suspects a security incident or data breach must immediately report the matter through one or more of the following channels:

- Their immediate supervisor;
- The Corporate Compliance Office; and/or
- Information Technology Services.

Reports must be made as soon as possible and must not be delayed for investigation or confirmation by the reporting individual.

Where possible, the report should include:

- Description of the incident or suspected breach;
- Type of data or systems involved;
- Date and time of discovery;
- Known or suspected source of the incident; and
- Any actions already taken.

Users must not attempt to investigate, remediate, or disclose the incident independently.

Incident Response and Coordination

Upon notification of a suspected or confirmed incident:

- Information Technology Services shall assess, contain, and investigate the technical aspects of the incident;
- The Corporate Compliance Office shall coordinate breach assessment, documentation, and regulatory response;

- The County Attorney shall be engaged, as appropriate, to determine legal obligations, notification requirements, and disclosure actions in accordance with applicable law; and
- Other departments or stakeholders may be engaged as necessary.

All response activities shall be coordinated to ensure accuracy, consistency, and compliance with legal and regulatory requirements.

Legal and Regulatory Compliance

All data breaches involving personal or private information shall be handled in accordance with applicable laws, including but not limited to:

- New York State General Business Law Section 899-aa;
- New York State Technology Law Section 208; and
- Any other applicable federal, state, or regulatory requirements.

The Corporate Compliance Office, in coordination with the County Attorney, shall determine whether notification is required and the appropriate method, timing, and scope of such notification.

Required reporting forms and documentation, including applicable New York State breach reporting forms, shall be completed as part of the response process.

Regulated Data Considerations

Where a security incident or data breach involves regulated data, additional legal and regulatory requirements shall apply.

Such data may include, but is not limited to:

- Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA);
- Substance Use Disorder (SUD) records protected under 42 CFR Part 2;
- Information governed under New York State Article 28 or other Department of Health regulations; and
- Any other data subject to federal, state, or contractual confidentiality requirements.

In such cases:

- The Corporate Compliance Office shall ensure that all applicable regulatory requirements are identified and followed;
- The County Attorney shall determine legal notification obligations;
- Information Technology Services shall support technical investigation and containment; and
- Additional reporting, notification, and documentation requirements shall be completed in accordance with applicable law and regulation.

Where regulatory requirements impose stricter standards than County policy, the stricter standard shall apply.

Confidentiality and Communication

Information related to a suspected or confirmed security incident or data breach shall be treated as confidential and shared only with authorized personnel.

Employees shall not:

- Disclose incident details to unauthorized individuals;
- Communicate with external parties, including the public or media, regarding the incident; or
- Provide statements or documentation without authorization.

All external communications shall be coordinated through appropriate County leadership in consultation with the County Attorney.

Preservation of Evidence

Users must take reasonable steps to preserve evidence related to a suspected incident, including:

- Not altering or deleting affected data;
- Not powering off affected systems unless directed; and
- Following instructions from Information Technology Services.

Preservation of evidence is critical for investigation, legal compliance, and potential enforcement actions.

Enforcement

Failure to comply with this policy, including failure to report a suspected incident, may result in disciplinary action, up to and including termination of employment, and/or legal action where applicable.

Disclaimer

Sullivan County assumes no liability for damages resulting from delayed or unreported incidents where such delay results from failure to comply with this policy, except as otherwise required by law.

SCITS-9030.001 Policy – Disaster Recovery & System Prioritization Standard

Title	Number
Disaster Recovery & System Prioritization Standard	**SCITS-9030.001**

Creation Date: **May 2026**

Modified Date:

Purpose

The purpose of this Standard is to define Sullivan County's system recovery prioritization framework, including Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), to support effective disaster recovery, cybersecurity incident response, and business continuity operations.

This Standard provides the operational detail required to execute system restoration in a consistent, risk-based, and prioritized manner in alignment with County policy.

Scope

This Standard applies to:

- All County-owned, County-managed, or County-supported systems and infrastructure;
- All systems included in the County's backup and disaster recovery program; and
- All environments, including on-premises, cloud, and hybrid systems.

Recovery Tier Definitions

Tier	Description	RTO (Recovery Time Objective)	RPO (Recovery Point Objective)
Tier 1 – Life Safety / Critical	Immediate impact to public safety or health	0–4 hours	Near-zero to <1 hour
Tier 2 – Essential Operations	Critical County operations or regulatory impact	4–24 hours	<4–8 hours
Tier 3 – Business Operations	Departmental operations and internal services	24–72 hours	<24 hours
Tier 4 – Non-Critical / Support	Low-impact or non-essential systems	3–7 days	24–72+ hours

System Recovery Prioritization Matrix

Tier 1 – Life Safety / Critical Systems

System	Description	RTO	RPO
911 / Public Safety Systems (CAD, Dispatch, Radio Interfaces)	Emergency response coordination systems	0–2 hours	Near-zero
Public Health Systems (Article 28 / PHS / EHR)	Clinical and patient care systems	2–4 hours	<1 hour

Tier 2 – Essential Operations

System	Description	RTO	RPO
Financial Systems (ERP, Payroll, Accounting)	Financial operations and payroll processing	8–24 hours	<4–8 hours
Law Enforcement / Records Systems (RMS, CJIS)	Criminal justice and records systems	8–24 hours	<4 hours
Email & Communications Systems	Internal and external communication platforms	4–12 hours	<4 hours
Core Network Infrastructure (AD, DNS, DHCP)	Identity, authentication, and network services	4–8 hours	<1–4 hours

Tier 3 – Business Operations

System	Description	RTO	RPO
File Servers / Shared Drives	Departmental file storage and collaboration	24–48 hours	<24 hours
Document Management / Records Systems	Records retention and retrieval systems	24–72 hours	<24 hours
Departmental Line-of-Business Applications	Case management, permitting, DSS systems	24–72 hours	<24 hours

Tier 4 – Non-Critical / Support Systems

System	Description	RTO	RPO
Reporting, Analytics, and Training Systems	Reporting tools, BI platforms, training environments	3–7 days	24–72+ hours

Operational Use

This recovery prioritization framework shall be used to:

- Guide system restoration sequencing during cybersecurity incidents or disasters;
- Support decision-making by the Incident Commander (CIO) during incident response;
- Align recovery efforts with business continuity priorities; and
- Ensure consistent and predictable recovery outcomes across the County.

During an incident, recovery shall generally proceed in the following order:

1. Core network and identity infrastructure
2. Life safety and public health systems

3. Essential operational systems
4. Business and departmental systems
5. Non-critical systems

The CIO retains authority to modify prioritization based on real-time incident conditions.

Governance and Maintenance

Information Technology Services shall:

- Maintain and update this Standard as systems, technologies, and operational priorities evolve;
- Review system classifications and RTO/RPO assignments at least annually;
- Update the matrix when new systems are introduced or existing systems are significantly modified; and
- Ensure alignment with County policies, regulatory requirements, and operational risk.

Exception Management

Any deviation from defined RTO/RPO targets or recovery prioritization must be:

- Documented;
- Approved by the CIO or designee; and
- Justified based on operational, technical, or risk considerations.

Relationship to Policy

This Standard provides the operational implementation of:

- Data Backup and Recovery Policy
- Incident Response and Cybersecurity Event Management Policy

In the event of conflict, County policy shall take precedence.

Section 10 — Operational and Administrative Controls (10000 Series)

SCITS-10000.001 – IT Service Request and Support Policy

Title	Number
IT Service Request and Support Policy	SCITS-10000.001

Creation Date: May 2026

Modified Date:

Purpose

The purpose of this policy is to establish standardized procedures for requesting Information Technology (IT) services and reporting incidents or problems affecting County systems.

Effective service request and incident reporting processes are essential to:

- Minimize disruption to County operations;
- Ensure timely resolution of technical issues;
- Enable proper tracking, prioritization, and scheduling of IT work; and
- Maintain consistent service expectations across all departments.

Scope

This policy applies to:

- All Sullivan County employees, elected officials, contractors, consultants, interns, and other authorized users; and
- All County-owned or supported systems, applications, infrastructure, and services.

All requests for IT services and all incidents affecting system availability, performance, or security must be reported through County-approved service management channels.

General Policy

All IT service requests and incident reports shall be submitted through the County's designated IT Service Management (ITSM) system (Help Desk), either directly by the user or through Information Technology Services.

The Commissioner of Information Technology / Chief Information Officer (CIO), or designee, has authority over:

- Prioritization of service requests and incidents;
- Allocation of IT resources;
- Scheduling of work; and
- Determination of response and resolution timelines.

All requests and incidents will be logged, tracked, and managed through the ITSM system to ensure accountability, visibility, and proper resolution.

Service Request and Incident Classification

All submissions will be categorized as one of the following:

- **Service Request**: A request for new service, equipment, access, or a standard change (e.g., new user setup, device request, configuration change).
- **Incident**: An unplanned interruption or degradation of service (e.g., system outage, application failure, connectivity issue).
- **Security Incident**: Any event involving suspected or confirmed compromise of systems, data, or accounts, which must also be reported in accordance with the County's Security Incident and Data Breach Reporting Policy.

Information Technology Services will assign priority levels based on business impact, urgency, and risk.

Submission of Requests and Incidents

All IT service requests and incidents must be submitted through approved channels, which may include:

- The County ITSM (Help Desk) system;
- Email or electronic submission methods designated by Information Technology Services; or
- Direct contact with the IT Help Desk for urgent or critical issues.

Users must provide sufficient detail to allow proper triage, including a description of the issue, affected systems or users, and any relevant timing or business impact.

Service Levels and Scheduling

Information Technology Services will:

- Review, prioritize, and assign all requests and incidents;
- Schedule work based on priority, resource availability, and operational impact; and
- Communicate status updates and resolution progress to the requestor.

Routine service requests and planned changes will generally be performed during standard business hours, unless otherwise approved.

Emergency or high-priority incidents may be addressed outside of normal business hours as required to restore service or mitigate risk.

Equipment Moves, Adds, and Changes

Requests involving the movement, addition, or modification of IT equipment or services must be submitted in advance whenever possible.

Information Technology Services will:

- Evaluate and schedule such requests to minimize disruption;
- Coordinate any required service interruptions; and
- Notify affected users of expected downtime where applicable.

While reasonable effort will be made to meet requested timelines, scheduling is subject to operational priorities and resource availability.

Incident Response Expectations

For incidents:

- Information Technology Services will initiate response based on assigned priority;
- Efforts will be made to restore service as quickly as possible; and
- Users will be informed of significant outages, expected resolution timelines, and service restoration.

Critical incidents affecting multiple users or essential services will receive highest priority.

User Responsibilities

Users are responsible for:

- Promptly reporting issues or service needs;
- Providing accurate and complete information;
- Cooperating with troubleshooting and resolution efforts; and
- Using County systems in accordance with all applicable policies.

Failure to report issues in a timely manner may result in extended service disruptions.

Monitoring and Reporting

All service requests and incidents will be tracked and documented within the ITSM system.

Information Technology Services may use this data to:

- Identify recurring issues;
- Improve service delivery;
- Support planning and resource allocation; and
- Provide reporting to County leadership.

Enforcement

Failure to follow established procedures for submitting service requests or reporting incidents may result in delays in service delivery and may be addressed through administrative action where appropriate.

Disclaimer

Sullivan County does not guarantee uninterrupted availability of IT services and is not liable for disruptions resulting from system failures, maintenance activities, or circumstances beyond its control.

SCITS-10030.001 Security Awareness, Training, and Testing

Title	Number
Security Awareness, Training, and Testing	**SCITS-10030.001**
Creation Date: **February 2021**	
Modified Date: **April 2026**	

Policy Statement

Sullivan County shall maintain a comprehensive, continuous Security Awareness, Training, and Testing Program to ensure that all personnel understand their information security responsibilities and are capable of recognizing and responding to evolving cybersecurity threats.

All workforce members, including employees, contractors, and authorized third parties, are required to participate in security awareness training and are subject to ongoing testing and evaluation as a condition of access to County information systems and data.

The program shall be risk-based, measurable, and enforceable, and shall support the County's broader information security, risk management, and compliance objectives.

Training Requirements

Mandatory Training

- All personnel shall complete security awareness training:
  - Upon initial onboarding; and
  - At least annually thereafter
- Training shall cover, at a minimum:
  - Acceptable use of County systems
  - Protection of sensitive and confidential information
  - Phishing, social engineering, and fraud awareness
  - Password and authentication security
  - Incident identification and reporting procedures

Role-Based Training

- Additional training shall be required for personnel with elevated access, specialized roles, or increased risk exposure, including but not limited to:

  - Information Technology staff
  - Security administrators
  - Finance and procurement personnel
  - Executives and elected officials
- Role-based training requirements shall be defined and maintained in coordination with departmental leadership.

Continuous Awareness

- Security awareness shall be reinforced through ongoing activities, which may include:
  - Periodic communications and advisories
  - Awareness campaigns
  - Targeted educational content based on emerging threats

Security Testing and Simulated Social Engineering

Testing Program

The County shall conduct periodic simulated social engineering exercises to evaluate user awareness and behavior.

Testing may include, but is not limited to:

- Phishing (email-based attacks)
- Vishing (voice-based attacks)
- Smishing (SMS/text-based attacks)
- Malicious media testing (e.g., USB devices)
- Physical security and social engineering assessments

Testing Approach

- Testing shall be conducted on a randomized and/or targeted basis
- Frequency, complexity, and targeting shall be determined based on risk
- High-risk individuals or groups may be subject to increased testing

User Actions and Outcomes

- User interactions during testing shall be evaluated to determine:
- Susceptibility to simulated attacks
- Proper identification and reporting of threats
- Compliance with County security policies

Remediation and Risk-Based Actions

- Personnel who demonstrate elevated risk through training or testing outcomes may be subject to:

    - Targeted or remedial training
    - Increased testing frequency
    - Direct coaching or intervention
- Repeated or significant risk indicators may result in additional administrative or technical safeguards, including restrictions or enhanced monitoring, as appropriate.

Compliance Monitoring and Metrics

- The County shall monitor and track:
    - Training completion rates
    - Testing participation and outcomes
    - Reporting rates of simulated and real threats
    - Trends in user behavior and risk
- Metrics shall be used to:
    - Assess program effectiveness
    - Inform risk management decisions
    - Support reporting to executive leadership

Enforcement

- Compliance with this policy is mandatory.
- Failure to complete required training or failure to adhere to security practices, including unsafe behavior identified during testing, may result in corrective actions.
- Corrective actions shall be risk-based, progressive in nature, and coordinated with Human Resources and applicable personnel policies.
- All corrective actions shall be administered in accordance with applicable personnel policies, collective bargaining agreements, and legal requirements.

Roles and Responsibilities

Commissioner of ITS / Chief Information Officer (CIO) / Information-Network Security Officer

- Establish and maintain the Security Awareness, Training, and Testing Program
- Ensure alignment with County policies, regulatory requirements, and risk management practices
- Report program effectiveness and risk posture to leadership

Information Technology Services (ITS)

- Develop, deliver, and manage training and testing activities
- Conduct simulated social engineering exercises
- Monitor participation, performance, and risk indicators

Department Heads and Management

- Ensure staff participation in required training and activities

- Support enforcement of policy requirements
- Reinforce security awareness within their departments

All Personnel

- Complete required training within established timeframes
- Actively participate in awareness and testing activities
- Adhere to all County information security policies and practices
- Promptly report suspected or actual security incidents

Integration with County Security Program

This program supports and is integrated with:

- Information Security Governance
- Risk Management
- Incident Response
- Acceptable Use
- Access Control and Identity Management

Results from awareness training and testing shall inform broader security controls, risk assessments, and continuous improvement efforts.

SCITS-10030.001-S1 Security Awareness Enforcement and Escalation Standard

Title	Number
Security Awareness Enforcement and Escalation Standard	**SCITS-10030.001-S1**

Creation Date: **February 2021**

Modified Date: **April 2026**

Purpose

This standard defines the enforcement model and escalation framework for non-compliance with the County's Security Awareness, Training, and Testing Program.

This standard supports **SCITS-3070.001 — Security Awareness, Training, and Testing Policy** and establishes a consistent, risk-based approach to addressing user behavior that increases cybersecurity risk.

Scope

This standard applies to all personnel, including employees, contractors, elected officials, and third parties with access to County systems, networks, or data.

Definitions

- **Non-Compliant Event**
  Any action or inaction that violates training or security awareness expectations, including but not limited to:
  - Failure to complete required training within defined timeframes
  - Unsafe interaction with a simulated social engineering exercise
- **Simulated Social Engineering Failure**
  Includes, but is not limited to:
  - Clicking malicious links in simulated phishing emails
  - Opening or executing malicious attachments
  - Submitting credentials or sensitive data
  - Responding to simulated vishing or smishing attempts
  - Interacting with malicious media (e.g., USB devices)
  - Failing to adhere to policy during physical social engineering exercises

- **Successful Security Behavior Event**
  Includes:
  - Proper identification and reporting of simulated or real threats
  - Appropriate non-interaction with malicious content

Enforcement Framework

General Principles

- Enforcement shall be:
  - Risk-based
  - Progressive
  - Consistent across the organization
  - Coordinated with Human Resources policies and procedures
  - Administered in accordance with applicable personnel policies, collective bargaining agreements, and legal requirements
- The objective of enforcement is to:
  - Reduce organizational risk
  - Improve user awareness and behavior
  - Reinforce accountability

Escalation Model

The County shall apply progressive corrective actions based on repeated or significant non-compliant events.

Level 1 — Initial Non-Compliance

Trigger:

- First failure of training completion or testing event

Actions:

- Mandatory completion of assigned training
- Automated or written notification

Level 2 — Repeated Non-Compliance

Trigger:

- Multiple non-compliant events within a defined period

Actions:

- Targeted remedial training
- Notification to supervisor or department management

Level 3 — Elevated Risk Behavior

Trigger:

- Continued non-compliance or demonstrated pattern of risky behavior

Actions:

- Formal review with department management
- Documented corrective action plan
- Increased testing frequency

Level 4 — High-Risk or Persistent Non-Compliance

Trigger:

- Repeated failures indicating elevated organizational risk

Actions:

- Escalation to senior leadership and Human Resources
- Consideration of administrative or technical controls, including:
- Access restrictions
- Enhanced monitoring
- Additional mandatory controls

Level 5 — Critical or Egregious Behavior

Trigger:

- Severe or repeated violations that present significant risk

Actions:

- Formal disciplinary review in accordance with County personnel policies
- Potential for suspension or termination of access or employment

Remediation and De-Escalation

- Remediation actions shall be assigned following non-compliant events and may include:
  - Training modules
  - Coaching sessions
  - One-on-one intervention
- De-escalation may occur when:
  - Personnel demonstrate sustained compliant behavior
  - Successful security behavior events are observed over time
- The County may reset or reduce escalation levels based on improved performance and reduced risk.

Exception Handling

- The ITS Division may determine that certain events are false positives or do not reflect actual risk and may exclude them from enforcement tracking.
- Exceptions shall be:
    - Documented
    - Justified
    - Subject to periodic review

Documentation and Reporting

- All non-compliant events, remediation actions, and escalation steps shall be documented.
- Summary reporting shall be provided to:
    - Department leadership
    - Executive leadership
    - Risk and governance functions

SCITS-10030.001-S2 — Security Awareness Risk Scoring Standard

Title	Number
Security Awareness Risk Scoring Standard	**SCITS-10030.001-S2**

Creation Date: **February 2021**

Modified Date: **April 2026**

Purpose

This standard defines the methodology for assessing and managing personnel risk related to security awareness and susceptibility to social engineering threats.

This standard supports targeted training, testing, and risk mitigation activities.

Scope

This standard applies to all personnel with access to County systems, networks, or data.

Risk Scoring Model

The County shall maintain a **dynamic user risk scoring model** that evaluates individuals based on behavioral, access-based, and contextual risk factors.

Risk scores shall be used to:

- Inform testing frequency and complexity
- Target training and remediation efforts
- Identify high-risk individuals or groups

Risk Factors

Risk scoring may include, but is not limited to, the following categories:

Behavioral Risk Indicators

- History of non-compliant events
- Repeated failures in simulated testing
- Failure to report suspicious activity

Access and Role-Based Risk

- Access to sensitive or confidential data
- Privileged or administrative system access
- Financial, procurement, or authorization authority
- Executive or elected official status (high-value targets)

Exposure Risk Indicators

- Inclusion in known data breach or credential exposure datasets
- Publicly available personal or professional information
- Use of County systems for external communication

Technology and Usage Risk

- Use of mobile devices for County business
- Remote access to County systems
- Use of non-standard or higher-risk endpoints

Policy and Security Posture Indicators

- Weak or non-compliant authentication practices
- Prior violations of County IT or security policies

Risk Levels

Personnel may be categorized into risk tiers, such as:

- **Low Risk** — Demonstrates consistent compliant behavior
- **Moderate Risk** — Occasional non-compliance or elevated exposure
- **High Risk** — Repeated failures or high-value access
- **Critical Risk** — Persistent behavior posing significant organizational risk

Risk-Based Actions

Risk levels shall inform:

- **Training Requirements**
  - Increased frequency or targeted modules
- **Testing Activities**
  - More frequent or sophisticated simulated attacks
- **Security Controls**
  - Enhanced monitoring
  - Conditional access or additional safeguards

Review and Adjustment

- Risk scores shall be:
    - Continuously updated based on behavior and activity
    - Reviewed periodically by ITS
- Adjustments shall be made based on:
    - Improved user behavior
    - Changes in role or access
    - Emerging threat intelligence

Data Handling and Privacy

- Risk scoring data shall be treated as sensitive internal information
- Access to risk data shall be limited to authorized personnel
- Use of risk data shall be strictly for security and risk management purposes

Appendix-A: Employee Information Security Policy Agreement

Acknowledgment of Information Security Responsibilities

I acknowledge that I have been provided access to the Sullivan County Information Technology Governance and Information Security Policies.

I understand that:

- County systems, devices, networks, and data are provided for authorized business use;
- I am responsible for protecting County information from unauthorized access, disclosure, or loss; and
- I am required to follow all applicable information technology and security policies.

User Account and Credential Security

I understand that:

- I will be assigned a unique user account (Network-ID) and authentication credentials;
- My account is for my use only and must not be shared; and
- I am responsible for all activity performed under my account.

I agree that I will:

- Keep my password and authentication methods (including MFA) confidential;
- Not share or allow others to use my account; and
- Immediately report any suspected compromise of my account.

Acceptable Use

I agree to:

- Use County systems and data only for authorized business purposes;
- Follow all policies related to email, internet use, mobile devices, and data storage; and
- Not attempt to bypass security controls or use unauthorized systems or services.

I further understand that, unless expressly authorized by Information Technology Services (ITS) for legitimate business purposes, **I shall not**:

System and Software Controls

- Install, download, or use unauthorized software, applications, or utilities;
- Modify system configurations, security settings, or system controls;
- Disable, bypass, or interfere with antivirus, endpoint protection, or other security mechanisms;

Hardware and Equipment Controls

- Install, modify, relocate, or remove County-owned hardware or peripherals;
- Swap or reassign equipment between systems without authorization;
- Remove County equipment from County premises without authorization (except for approved mobile devices);
- Accept or connect non-County equipment to County systems without authorization;

System Configuration and Integrity

- Alter system settings, configurations, or user environments beyond what is authorized for my role;
- Modify system interfaces (such as desktop configurations or system access points) in a manner that interferes with standard operations or support;

Data, Internet, and Email Use

- Download, open, or distribute files, applications, or attachments that may pose a security risk;
- Use unauthorized external media or storage devices without appropriate security validation;
- Use County email or internet access for non-business purposes beyond incidental personal use permitted by policy;
- Access, download, or transmit inappropriate, unlawful, or non-business-related content;

General Misuse

- Use County systems for any purpose that is unlawful, disruptive, or inconsistent with County operations or policy.

These restrictions reflect baseline security and operational controls and may be adjusted or authorized by ITS where necessary to support legitimate business needs.

Monitoring and Use of Systems

I understand that:

- Sullivan County systems and networks may be monitored, logged, and reviewed; and
- I have no expectation of privacy when using County systems or devices, except as otherwise provided by law.

Reporting Responsibilities

I agree to immediately report:

- Suspicious emails, activity, or system behavior;

- Lost or stolen devices; and
- Any known or suspected security incident or policy violation.

Enforcement

I understand that:

- Access to County systems is a privilege and may be modified or revoked at any time;
- Systems may be restricted to authorized configurations and software to maintain security and compliance; and
- Failure to comply with County policies may result in disciplinary action, up to and including termination, and potential legal consequences.

Acknowledgment

By signing below, I confirm that I understand my responsibilities and agree to comply with Sullivan County information security requirements.

This acknowledgment does not alter or supersede applicable personnel policies, collective bargaining agreements, or legal rights and obligations.

_____

Employee Name (Printed)

_____

Employee Signature Date

_____

Department

Appendix B — Equipment Use and Acknowledgment Agreement

Sullivan County, New York

My signature below acknowledges that I have been issued a Sullivan County–owned device ("Device"), which may include, but is not limited to, a mobile phone, tablet, laptop computer, or other electronic equipment.

Ownership and Use

The Device remains the sole property of Sullivan County and is provided for authorized County business purposes. All use of the Device must comply with applicable County policies, including but not limited to the Acceptable Use Policy, Information Security Policy, and Mobile Device Policy.

Limited Personal Use

Incidental personal use, if permitted, must be minimal, must not interfere with County operations, and must not violate any County policy or applicable law.

No Expectation of Privacy

Users have **no expectation of privacy** in any data stored on or transmitted through County-owned devices. Sullivan County reserves the right to monitor, access, audit, and disclose all activity and data on the Device at any time, with or without notice, in accordance with applicable law.

Security and Protection

I agree to:

- Safeguard the Device from loss, theft, or unauthorized access
- Not share passwords or access credentials
- Not disable or circumvent security controls, monitoring tools, or management software
- Use only software and applications approved by Information Technology

Device Management and Control

I acknowledge that the Device may be remotely managed, monitored, restricted, or wiped by Sullivan County Information Technology at any time, including in the event of loss, theft, policy violation, or separation of employment.

Loss, Theft, or Damage

I agree to immediately report any loss, theft, or damage of the Device to my Department Head and Information Technology. Failure to do so may result in disciplinary action.

Prohibited Actions

I agree not to:

- Install or remove unauthorized software
- Alter system configurations or security settings
- Remove County accounts, profiles, or management controls

Return of Equipment

Upon request or upon termination of employment, I agree to immediately return the Device in good working condition, reasonable wear and tear excepted.

Enforcement

Failure to comply with this Agreement or applicable County policies may result in disciplinary action, up to and including termination of employment, as well as potential civil or criminal penalties where applicable.

_____

Employee Name (Printed)

_____

Employee Signature Date

_____

Department

Device: _____

Inventory Tag: _____

Appendix-C: CJIS Compliance Summary

Executive Summary

Sullivan County recognizes that law enforcement operations require timely, secure, and reliable access to Criminal Justice Information (CJI) in order to support public safety, reduce crime, and ensure effective administration of justice. In support of these objectives, the County adheres to the requirements of the **Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy**, as established through the CJIS Advisory Policy Board (APB).

The CJIS Security Policy defines the minimum-security requirements for protecting CJI across its entire lifecycle, including the creation, access, transmission, storage, dissemination, and destruction of such information. These requirements apply to all individuals and entities—whether County employees, contractors, vendors, or partner agencies—who access, manage, or support systems containing CJI.

The County acknowledges that CJIS compliance is not limited to law enforcement systems alone, but extends to all supporting infrastructure, including hardware, software, networks, cloud or hosted services, and administrative processes that store, process, or transmit CJI. Accordingly, Sullivan County enforces CJIS-aligned administrative, technical, and physical controls across all applicable systems and environments.

The CJIS Security Policy is grounded in federal law, including the Federal Information Security Management Act (FISMA), as well as guidance from the National Institute of Standards and Technology (NIST). It establishes a standardized framework for risk management and security controls while allowing agencies to implement additional safeguards based on operational needs and risk tolerance.

Sullivan County maintains a shared responsibility model for CJIS compliance, working in coordination with the designated CJIS Systems Agency (CSA), State Identification Bureau (SIB), and other authorized entities, as applicable. All systems, users, and processes within the County that interact with CJI must comply with CJIS requirements, and are subject to audit, monitoring, and enforcement.

The County further recognizes that CJIS compliance is an ongoing operational obligation. Policies, procedures, and technical controls are reviewed and updated as necessary to address evolving threats, regulatory changes, and advancements in technology, while maintaining alignment with CJIS standards.

Nothing in this appendix limits the authority of the Commissioner of Information Technology / Chief Information Officer to implement and enforce additional safeguards, restrictions, or controls necessary to ensure CJIS compliance and protect County systems and data.

The complete CJIS Security Policy is maintained by the FBI and is available at:
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

Appendix-D: PCI Compliance Executive Summary

Sullivan County recognizes its responsibility to protect payment card data and to maintain a secure environment for all systems that accept, process, transmit, or otherwise interact with cardholder information. In support of this obligation, the County adheres to the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS establishes a comprehensive set of administrative, technical, and physical security requirements designed to protect cardholder data and reduce the risk of fraud, data breaches, and unauthorized disclosure. These requirements apply to all County departments, systems, personnel, vendors, and third-party service providers involved in payment processing activities, regardless of the method of acceptance (e.g., in-person, online, or third-party hosted solutions).

The PCI DSS is developed and maintained by the Payment Card Industry Security Standards Council (PCI SSC), an independent organization founded by the major payment card brands, including Visa, MasterCard, American Express, Discover, and JCB. While the PCI SSC establishes the standards, compliance enforcement is carried out by the payment brands and acquiring financial institutions.

Sullivan County maintains a risk-minimization approach to PCI compliance. To the greatest extent practicable, the County limits its exposure to cardholder data by utilizing third-party, PCI-compliant payment processors and ensuring that cardholder data is not stored, processed, or transmitted on County-owned systems unless explicitly authorized and secured in accordance with PCI DSS requirements.

All County systems and networks that connect to or support payment processing environments are subject to PCI DSS controls, including but not limited to network segmentation, access control, logging and monitoring, vulnerability management, and secure configuration standards. Any system determined to be within the scope of PCI DSS is subject to review, restriction, or remediation as directed by the Commissioner of Information Technology / Chief Information Officer.

The Commissioner of Information Technology / Chief Information Officer retains authority to define PCI scope, approve or prohibit payment processing methods, require architectural changes, and enforce technical and administrative controls necessary to achieve and maintain compliance. No County department may implement, modify, or expand payment processing capabilities without prior written approval from Information Technology and adherence to County procurement, security, and compliance requirements.

PCI compliance is an ongoing operational requirement. Departments that accept payments are responsible for coordinating with Information Technology, the County Treasurer, and other applicable oversight functions to ensure continued compliance, including completion of required self-assessment questionnaires (SAQs), maintenance of compliant vendor relationships, and adherence to all applicable security controls.

Nothing in this appendix limits the County's authority to impose stricter controls than those required by PCI DSS where necessary to protect County systems, financial operations, and public trust.

Additional information regarding PCI DSS requirements can be found at:
https://www.pcisecuritystandards.org/

Definitions and Acronyms

Authentication: The process of verifying the identity of a user, device, or system using one or more authentication factors (e.g., password, token, biometric).

Authorization: The process of granting or denying access to systems, data, or resources based on an authenticated identity and assigned permissions.

Availability: The condition in which information systems and data are accessible and usable upon demand by authorized users.

Biometric Data: Unique physical or behavioral characteristics (e.g., fingerprint, facial recognition, voice pattern) used to verify identity.

BYOD (Bring Your Own Device): Personally owned devices authorized for use to access County systems or data, subject to County security controls and approval.

Classification (Data Classification): The process of categorizing information based on sensitivity, regulatory requirements, and risk to determine appropriate protections.

CIA Triad: A foundational information security model consisting of confidentiality, integrity, and availability.

CJIS (Criminal Justice Information Services): The FBI division and associated security policy governing the protection of Criminal Justice Information (CJI).

Confidentiality: The protection of information from unauthorized access or disclosure.

Controls (Security Controls): Administrative, technical, and physical safeguards implemented to reduce risk and protect information systems and data.

Copyright: Legal protection granted to creators of original works, providing exclusive rights to use, reproduce, and distribute those works.

Cryptography / Cryptographic Controls: Methods used to protect information through encryption and related techniques to ensure confidentiality and integrity.

Cryptographic Key: A value used in cryptographic algorithms to encrypt or decrypt data.

Data: See **Information**.

Data Breach (Security Breach): The unauthorized acquisition, access, use, or disclosure of sensitive, confidential, or regulated information.

Denial of Service (DoS / DDoS): An attack that disrupts system or network availability by overwhelming resources.

DMZ (Demilitarized Zone): A segmented network zone that isolates external-facing systems from internal County networks.

Electronic Storage Media: Any digital storage medium, including hard drives, solid-state drives, removable media, and cloud storage platforms.

Encryption: The transformation of data into a secure format to prevent unauthorized access.

Firewall: A security system that monitors and controls network traffic based on defined security rules.

HIPAA (Health Insurance Portability and Accountability Act): Federal law governing the protection of Protected Health Information (PHI).

Host: Any device (e.g., server, workstation, virtual machine) connected to a network that stores or processes data.

Identity: A unique representation of a user, system, or device within an information system.

Incident (Security Incident): Any event that compromises or threatens the confidentiality, integrity, or availability of information systems or data.

Incident Response: The structured process for detecting, responding to, containing, and recovering from security incidents.

Information: Any data, regardless of form or medium, created, received, stored, or transmitted in support of County operations.

Information Asset: Any data, system, or resource that has value to the County and requires protection.

Information Custodian: The entity responsible for the day-to-day management and protection of information on behalf of the owner (typically IT).

Information Owner: The individual or department responsible for defining access, classification, and use of specific data.

Information Security: The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Integrity: The assurance that information is accurate, complete, and has not been altered without authorization.

Intranet: A private internal network accessible only to authorized County users.

Internet: A global network of interconnected systems used for communication and data exchange.

Intrusion Detection / Prevention (IDS/IPS): Systems that monitor and analyze network activity to detect and prevent malicious activity.

ISO (Information Security Officer): An individual responsible for implementing and overseeing security practices within a defined scope.

Malware: Malicious software designed to disrupt, damage, or gain unauthorized access to systems (e.g., ransomware, viruses, spyware).

Multi-Factor Authentication (MFA): An authentication method requiring two or more verification factors (e.g., password + DUO push, token, or phone verification).

Network ID (User Account): A unique identifier assigned to an individual for access to County systems.

Passphrase: A longer, more secure alternative to a password, typically consisting of multiple words.

PCI DSS (Payment Card Industry Data Security Standard) : A set of security standards for protecting payment card data.

Penetration Testing: A controlled security test that simulates real-world attacks to identify vulnerabilities.

Personal, Private, or Sensitive Information (PPSI): Information that, if disclosed, could harm individuals or the County, including personally identifiable information (PII), financial data, and security-sensitive information.

Protected Health Information (PHI): Health-related information that identifies an individual and is protected under HIPAA.

Phishing: A form of social engineering where attackers attempt to trick users into revealing sensitive information.

Privacy: The right to control how personal information is collected, used, and disclosed.

Privileged Account: An account with elevated permissions (e.g., administrator access) requiring additional security controls.

Ransomware: A type of malware that encrypts or blocks access to data or systems until a ransom is paid.

Remote Access: Access to County systems from outside the County network using approved secure methods.

Risk: The potential for loss or harm resulting from a threat exploiting a vulnerability.

Risk Assessment: The process of identifying, analyzing, and evaluating risks.

Risk Management: The process of identifying, assessing, and mitigating risks to acceptable levels.

Role-Based Access Control (RBAC): A method of restricting system access based on a user's role or job function.

Security Incident: See **Incident**.

Security Monitoring: Continuous observation of systems and networks to detect security events and anomalies.

Security Governance: The formal framework through which the County establishes authority, accountability, decision-making, and oversight for cybersecurity risk management, including the designation of the Chief Information Officer as the authoritative lead for cybersecurity operations and control enforcement.

Sensitive Information: Information requiring protection due to legal, regulatory, or operational risk.

Social Engineering: Techniques used to manipulate individuals into divulging confidential information.

Social Media: Internet-based platforms used for communication and content sharing.

Standard: A mandatory requirement that specifies how policies are implemented.

System: Any combination of hardware, software, and network components used to process information.

Third Party: Any external entity (vendor, contractor, consultant, partner) with access to County systems or data.

Threat: Any circumstance or event that could exploit a vulnerability and cause harm.

Unauthorized Access: Access to systems or data without proper authorization.

User: Any authorized individual accessing County systems or data.

Vulnerability: A weakness that could be exploited to compromise security.

Vulnerability Scanning: Automated identification of security weaknesses in systems or applications.

Workforce: All employees, contractors, and individuals performing work on behalf of the County.

Zero Trust: A security model that assumes no implicit trust and requires continuous verification of users, devices, and access requests.

Contact Information

Questions concerning this guideline or requests for changes may be directed to:

Commissioner/Chief Information Officer
Division of Information Technology Services
Sullivan County Government Center
100 North Street
Monticello, New York 12701
845-807-0110
helpdesk@sullivanny.gov

File #: ID-8364 **Agenda Date:** 5/21/2026 **Agenda #:** 12.

Narrative of Resolution:
Over time, as the county highway system has been improved and in places realigned, portions of the old road, as it existed prior to reconstruction, have been made useless. This resolution authorizes, pursuant to Section 118 -a of the highway law, the County to execute a quitclaim deed, abandoning said unused or useless portions of the old road, to the abutting owner of record, at no cost to the County.

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: N/A

Are funds already budgeted? N/A

If 'Yes,' specify appropriation code(s):

If 'No,' specify proposed source of funds:

Specify Compliance with Procurement Procedures:

N/A

RESOLUTION INTRODUCED BY THE PUBLIC WORKS COMMITTEE TO ABANDON A PORTION OF FORMER COUNTY ROAD NO. 179 AND CONVEY SAME TO THE ABUTTING LANDOWNER

WHEREAS, The County Superintendent of Highways has provided for the reconstruction of a portion of County Road 179 as shown on plans entitled, "Land to be acquired for the Liberty-Countyline Pt. 2, State Highway No. 4, Sullivan County, Section No. 13 (April 9, 1912)"; and

WHEREAS, that portion of the old road, as it existed prior to the reconstruction, has been made useless as a result of the reconstruction and has, in fact, been abandoned as a County Road by virtue of said road reconstruction; and

WHEREAS, Parcel 1B (on the attached survey Exhibit "A") is a portion of Parcel "B" as shown on Map 20 of the aforementioned Liberty-Countyline Pt. 2 acquisition map, same having being acquired in fee from Oland Sherwood; and

WHEREAS, Parcel 2B (on the attached survey Exhibit "A") is a portion of the old highway, having since been relocated, same being a right-of-way (or highway) by use; and

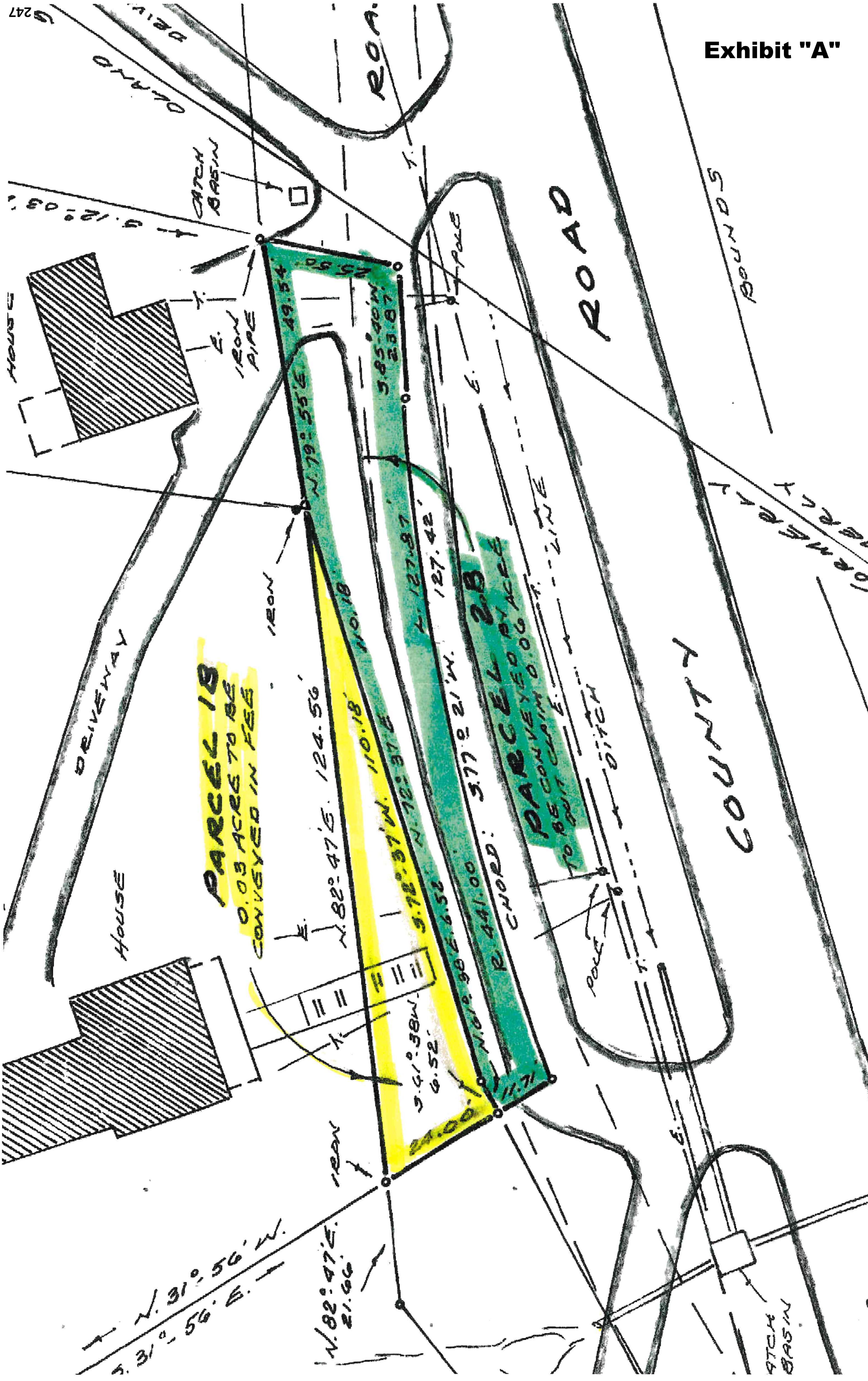
WHEREAS, pursuant to Section 118-a of the Highway Law and upon recommendation of the County Superintendent of Highways, the Chair of the Legislature is authorized to execute a Quitclaim Deed, in the name of the County, of the land so abandoned and to deliver the same, to the abutting owner(s), Glenn Johnson and Thomas Couteau (Town of Rockland Tax Lots; 24.-1-20 and 24.-1-22.1), for such consideration and upon such terms and conditions, as the County Legislature shall deem proper; and

WHEREAS, said Glenn Johnson and Thomas Couteau, as the abutting owner(s), have requested the County to abandon to them, that portion of the former right of way which is of no further use for highway purposes; and

NOW, THEREFORE, BE IT RESOLVED, that the Chair of the County Legislature is hereby authorized to execute, in the name of the County, a Quitclaim Deed of the land so abandoned and to deliver the same to, Glenn Johnson and Thomas Couteau, for no monetary consideration; and

BE IT FURTHER RESOLVED, that the Grantee will provide the appropriate legal description necessary and as requested by the County, at his cost and expense.

Exhibit "A"


PARCEL 1B
0.03 ACRES TO BE CONVEYED IN FEE
PARCEL 2B
TO BE CONVEYED BY QUIT CLAIM 0.06 ACRE
COUNTY ROAD
DRIVEWAY
HOUSE
HOUSE
CATCH BASIN
IRON PIPE
IRON
IRON
POLE
POLE
DITCH
T. LINE
N. 79° 55' E. 49.54
S. 85° 40' W. 23.87
25.50
N. 82° 47' E. 124.56
S. 72° 37' W. 110.18
N. 72° 37' E. 110.18
S. 77° 21' W. 127.42
127.97
R. 441.00
CHORD: S. 77° 21' W.
N. 61° 30' E. 6.52
S. 61° 38' W. 6.52
24.00
11.71
N. 82° 47' E. 21.66
N. 31° 56' W.
S. 31° 56' E.
CATCH BASIN

File #: ID-8365 **Agenda Date:** 5/21/2026 **Agenda #:** 13.

Narrative of Resolution:
TO AUTHORIZE A PAYMENT TO THOMSON REUTERS
If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $2,100.89

Are funds already budgeted? Choose an item.

If 'Yes,' specify appropriation code(s): A-1680-43-4304

If 'No,' specify proposed source of funds: N/A

Specify Compliance with Procurement Procedures: N/A

RESOLUTION INTRODUCED BY THE MANAGEMENT & BUDGET COMMITTEE TO AUTHORIZE PAYMENT TO THOMSON REUTERS

WHEREAS, by Resolution No. 337-22 adopted August 18, 2022, the Sullivan County Legislature authorized a three (3) year agreement with Thomson Reuters for the provision of subscription-based legal research services; and

WHEREAS, by Resolution No. 350-25 adopted August 21, 2025, the Legislature authorized a subsequent three (3) year continuation of said services; and

WHEREAS, due to delays in vendor processing of the continuation order, including approvals and execution, the effective date of the renewed agreement was established based upon the vendor's order processing date, resulting in a gap between agreements; and

WHEREAS, during the interim period of September through November 2025, the County continued to utilize the services to maintain operational continuity; and

WHEREAS, invoices totaling $2,100.89 were incurred for services rendered during this gap period; and

WHEREAS, payment of these invoices is necessary to satisfy the County's obligation for services received during the transition between agreements;

NOW, THEREFORE, BE IT RESOLVED, that the Sullivan County Legislature hereby authorizes the Sullivan County Audit Department to process payment to Thomson Reuters in an amount not to exceed $2,100.89 for invoices associated with services rendered during the period of September through November 2025, representing a bridge gap between authorized agreements; and

BE IT FURTHER RESOLVED, that such payment is made to satisfy the County's obligation for services received and utilized to maintain continuity of operations during the transition between agreements.

File #: ID-8366 **Agenda Date:** 5/21/2026 **Agenda #:** 14.

Narrative of Resolution:
TO AUTHORIZE A 3-YEAR AGREEMENT FOR CONTINUED ACCESS TO LEXISNEXIS ADVANCE ONLINE LEGAL RESEARCH PRODUCTS

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $78,408.00 (3-year total)

Are funds already budgeted? Yes

If 'Yes,' specify appropriation code(s): A-1680-43-4304

If 'No,' specify proposed source of funds: N/A

Specify Compliance with Procurement Procedures: Long-established vendor - renewal agreement and quote received.

RESOLUTION INTRODUCED BY THE MANAGEMENT & BUDGET COMMITTEE TO AUTHORIZE A 3-YEAR AGREEMENT FOR CONTINUED ACCESS TO LEXISNEXIS ADVANCE ONLINE LEGAL RESEARCH PRODUCTS

WHEREAS, Resolution No. 157-14, 223-17, 274-20, and 172-23 adopted by the Sullivan County Legislature on April 24, 2014, May 18, 2017, July 23, 2020 and April 20, 2023 respectively, authorized 3-year agreements for LexisNexis computer based legal search engine services with Lexis for Microsoft Office to reduce costs by eliminating redundant expenses for paper subscription services; and

WHEREAS, our current agreement with LexisNexis expires on 05/31/2026; and

WHEREAS, LexisNexis has performed as agreed over the past 12 years for departments such as the District Attorney, County Attorney and DFS Legal; and

WHEREAS, the County of Sullivan wishes to continue utilizing LexisNexis computer based legal research services including Lexis+ and Lexis for Microsoft Office.

NOW, THEREFORE, BE IT RESOLVED, that the County Manager is hereby authorized to enter into a 3-year agreement with LexisNexis for their Lexis+ Subscription Service and Lexis for Microsoft Office, for a total cost not to exceed $78,408.00 paid in 36 monthly installments as defined by their agreement of $2,178.00.

BE IT FURTHER RESOLVED, that said agreements to be in such form as the County Attorney shall approve.

File #: ID-8367 **Agenda Date:** 5/21/2026 **Agenda #:** 15.

Narrative of Resolution:
TO AUTHORIZE A NEW THREE-YEAR AGREEMENT WITH THOMSON REUTERS FOR THEIR "CLEAR" RESEARCH PRODUCT FOR THE BENEFIT OF THE DISTRICT ATTORNEY'S OFFICE

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $3,518.16 (3-year total)

Are funds already budgeted? Yes

If 'Yes,' specify appropriation code(s): A-1680-43-4304

If 'No,' specify proposed source of funds: N/A

Specify Compliance with Procurement Procedures: Long-established solution provider - 12+ years - new agreement and quote received.

RESOLUTION INTRODUCED BY THE MANAGEMENT & BUDGET COMMITTEE TO AUTHORIZE A NEW THREE-YEAR AGREEMENT WITH THOMSON REUTERS FOR THEIR "CLEAR" RESEARCH PRODUCT FOR THE BENEFIT OF THE DISTRICT ATTORNEY'S OFFICE

WHEREAS, the County of Sullivan wishes to enter into a three-year agreement with Thomson Reuters for its CLEAR web product to enable the County to perform research pertaining to fraud and other matters for the benefit of the District Attorney's Office; and

WHEREAS, the County is satisfied with the CLEAR web product and believes that the product will benefit the investigations of the Sullivan County District Attorney's Office.

NOW THEREFORE BE IT RESOLVED, the County Manager is hereby authorized to enter into a three-year agreement with Thomson Reuters for an amount not to exceed $3,518.16, subject to annual budget appropriation, as follows:

2026-2027	$1,116.00
2027-2028	$1,171.80
2028-2029	$1,230.36

BE IT FURTHER RESOLVED, that said agreement to be in such form as the County Attorney shall approve.

File #: ID-8369 **Agenda Date:** 5/21/2026 **Agenda #:** 16.

Narrative of Resolution:
Sullivan County Division of Public Works (DPW) requires crane services to construct various public works projects. This resolution will authorize the County Manager to execute an agreement for crane rental services with operator by as set forth in Bid B-26-23.

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $25,000.00

Are funds already budgeted? No

If 'Yes,' specify appropriation code(s):

If 'No,' specify proposed source of funds: D5110-46-47.4701 & D5110-46-40.4038

Specify Compliance with Procurement Procedures:

B-26-23

RESOLUTION INTRODUCED BY THE PUBLIC WORKS COMMITTEE TO AUTHORIZE THE COUNTY MANAGER TO EXECUTE A CONTRACT WITH PAYNE'S CRANES, INC. FOR CRANE SERVICES NEEDED FOR VARIOUS PUBLIC WORKS PROJECTS ON AN AS NEEDED BASIS

WHEREAS, Sullivan County Division of Public Works (DPW) requires crane services to construct various public works projects; and

WHEREAS, Bid B-26-23 was issued for crane rental with operator services, and Payne's Cranes, Inc. was the lowest qualified bidder for crane rental services with operator; and

WHEREAS, the Sullivan County Division of Public Works (DPW) recommends that an agreement be executed with Payne's Cranes, Inc for these services.

NOW, THEREFORE, BE IT RESOLVED, that the County Manager be and hereby is authorized to execute a contract for a one year period commencing June 1, 2026 through May 31, 2027 with the option to extend on a yearly basis for four additional years upon mutual agreement with Payne's Cranes, Inc at a cost not to exceed $25,000.00 in accordance with Sullivan County Bid B-26-35, in such form as the County Attorney shall approve.

File #: ID-8370 **Agenda Date:** 5/21/2026 **Agenda #:** 17.

Narrative of Resolution:
Resolution to authorize the County Manager to execute a modification agreement for engineering design services with McFarland Johnson for the 2026 Bridge Maintenance Project (PIN 9755.12)

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $56,317.00

Are funds already budgeted? Yes

If 'Yes,' specify appropriation code(s): D-5020-40-4006

If 'No,' specify proposed source of funds:

Specify Compliance with Procurement Procedures:

N/A

RESOLUTION INTRODUCED BY PUBLIC WORKS COMMITTEE TO AUTHORIZE A MODIFICATION TO THE ENGINEERING SERVICES AGREEMENT WITH MCFARLAND JOHNSON, INC. FOR THE 2026 SULLIVAN COUNTY BRIDGE MAINTENANCE PROJECT - SCOUR REPAIR PROJECT.

WHEREAS, the 2026 Sullivan County Bridge Maintenance Project, P.I.N. 9755.12 (the Project) located in the Towns of Callicoon and Liberty is to be implemented by contract and must meet the requirements of the NYSDOT Local Projects Manual; and

WHEREAS, Resolution No. 255-25 previously authorized an engineering services contract with McFarland Johnson, Inc for the design of the project; and

WHEREAS, additional engineering services are required to prepare additional plans, maps, and permit documents for the Project; and

WHEREAS, Resolution 140-26 authorized a Supplemental Agreement with NYSDOT to increase available funding from NYSDOT as the Project is eligible for 80% Federal and 15% State funding through the Bridge Maintenance and Marchiselli funding programs; and

WHEREAS, the Division of Public Works recommends a modification to the agreement with McFarland Johnson, Inc. for the additional work needed for the Project;

NOW, THEREFORE, BE IT RESOLVED, that Resolution 255-25 is hereby amended to add $56,317.00 to the original Agreement cost of $147,981.00; and

BE IT FURTHER RESOLVED, that the County Manager is authorized to execute a Modification Agreement with McFarland Johnson, Inc. for engineering services at a cost not to exceed $56,317.00 thereby increasing the contract maximum amount payable to $204,298.00, and said Agreement Modification shall be in such form as the County Attorney shall approve.

File #: ID-8371 **Agenda Date:** 5/21/2026 **Agenda #:** 18.

Narrative of Resolution:
Resolution to authorize award and execution of agreement for Cleaning of Leachate Storage Tanks at the Sullivan County Landfill to TAM Enterprises Inc., the lowest responsible bidder for the project.

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $9,600.00

Are funds already budgeted? Yes

If 'Yes,' specify appropriation code(s): CL-8160-47-4717

If 'No,' specify proposed source of funds:

Specify Compliance with Procurement Procedures:

N/A

RESOLUTION INTRODUCED BY PUBLIC WORKS COMMITTEE TO AUTHORIZE THE COUNTY MANAGER TO EXECUTE AN AGREEMENT FOR THE CLEANING OF THE LEACHATE STORAGE TANKS AT THE SULLIVAN COUNTY PRETREATMENT PLANT

WHEREAS, bids were received for the Cleaning of the Leachate Storage Tanks at the Sullivan County Pretreatment Plant; and

WHEREAS, TAM Enterprises, Inc. 114 Harley Road Goshen, NY 12924, is the lowest responsible bidder for this project; and

WHEREAS, the Sullivan County Division of Public works has approved said bid and recommends that an agreement be executed.

NOW, THEREFORE, BE IT RESOLVED, that the County Manager be and hereby is authorized to execute an agreement with TAM Enterprises, Inc., at an annual price based on $0.21/gallon and $675 per hour for the Cleaning of the Leachate Storage Tanks at the Sullivan County Pretreatment Plant, B-26-17, for the contract period June 1, 2026 through May 31, 2027, with four (4) additional yearly extensions, under the same terms and conditions, said contract to be in such form as the County Attorney shall approve; and

BE IT FURTHER RESOLVED, that the County Manager be and hereby is authorized to execute an agreement with TAM Enterprises, Inc., at a daily price not to exceed $13,200.00 for the unlikely Emergency Removal of raw Leachate in the event of a plant failure, B-26-17, for the contract period June 1, 2026 through May 31, 2027, with four (4) additional yearly extensions, under the same terms and conditions, said contract to be in such form as the County Attorney shall approve.

File #: ID-8373 **Agenda Date:** 5/21/2026 **Agenda #:** 19.

Narrative of Resolution:
Sullivan County Sheriff Admin & Jail facility requires fire alarm upgrade due to current system becoming obsolete, and parts being difficult or impossible to procure.

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $150,000.00

Are funds already budgeted? No

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: A1620-213-21-2102

Specify Compliance with Procurement Procedures:

NYS OGS Contract - (Group 77201 - Intelligent Facility and Security Systems & Solutions; Award Number - 23150; FS&S OGS Contract Number - PT68795; NYS Vendor ID - 1000031076)

RESOLUTION INTRODUCED BY THE PUBLIC WORKS COMMITTEE TO AUTHORIZE THE COUNTY MANAGER TO EXECUTE AN AGREEMENT WITH FIRE SECURITY & SOUND, INC. ("FS & S") TO PROVIDE REPAIR/UPGRADE SERVICES TO THE SOON TO BE OBSOLETE FIRE ALARM SYSTEM AT THE SHERIFF ADMINISTRATION AND JAIL FACILITY.

WHEREAS, the Sullivan County Sheriff Administration and Jail facility has complex fire alarm, sprinkler, and fire suppression systems, all of which require NYS Building Code mandated testing, inspection, and service on prescribed intervals (Fire Alarm: annual; Sprinkler: quarterly; Fire Suppression: semi-annual); and

WHEREAS, these systems are technically specialized and demand servicing which is required to be satisfactory to the product manufacturers; and

WHEREAS, the firm of Fire Security & Sound, Inc., 4 Avis Drive, Suite 110, Latham, NY 12110 was the subcontractor on the Jail construction project which installed these various systems and has intimate knowledge of the equipment, its functions, and locations, and has been performing the Inspection, Testing, & Service, as well as required system maintenance, since the commissioning of the facility; and

WHEREAS, due to the recent need for some significant repairs it has been brought to the County's attention that the existing fire alarm system will be obsolete at the end of 2026, and requires upgrading as service and parts will no longer be available; additionally, any necessary upcoming repair parts may prove impossible to procure prior to the end of 2026; and

WHEREAS, Fire Security & Sound, Inc. has the ability to provide the required upgrade as a vendor on New York State Contract, (Group 77201 - Intelligent Facility and Security Systems & Solutions; Award Number - 23150; FS&S OGS Contract Number - PT68795; NYS Vendor ID - 1000031076), and has provided a proposal based on this pricing for the upgrade work; and

WHEREAS, DPW Recommends a contract be executed in an amount not to exceed $150,000 with Fire Security & Sound South, Inc. for this required upgrade.

NOW, THEREFORE, BE IT RESOLVED, that the County Manager be and hereby is authorized to execute any and all agreements to retain the services of Fire Security & Sound, Inc. for the Sheriff Administration and Jail Facility Fire Alarm Repair/Upgrade, in the amount not to exceed $150,000, in such form as the County Attorney shall approve.

File #: ID-8375 **Agenda Date:** 5/21/2026 **Agenda #:** 20.

Narrative of Resolution:
Resolution to authorize amendments to Section 620.1 of the Sullivan County Solid Waste Management Rules.

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: N/A

Are funds already budgeted? N/A

If 'Yes,' specify appropriation code(s):

If 'No,' specify proposed source of funds:

Specify Compliance with Procurement Procedures:

N/A

RESOLUTION INTRODUCED BY THE EXECUTIVE COMMITTEE AUTHORIZING THE REVISION OF SECTION 620.1 OF THE SOLID WASTE MANAGEMENT RULES TO TAKE EFFECT ON JUNE 1, 2026

WHEREAS, the Sullivan County Solid Waste Management Rules (hereinafter the Rules) were adopted by the County Legislature in accordance with Section 171-24 of the Sullivan County Code; and

WHEREAS, from time to time it is necessary to adjust rates based on items such as but not limited to contract obligations, CIP increases and equitable distribution of actual costs; and

WHEREAS, a discussion has occurred in the Public Works Committee regarding the tipping rates. Specifically, Section 620.1 for the Construction and Demolition (C&D) rate to be lowered to $135.00 to try to get C&D that is leaving the County to come thru the Sullivan County Tip Floor. The Rules are attached with a markup to section 620.1 of the necessary changes.

NOW, THEREFORE, BE IT RESOLVED, the Solid Waste Management Rules be modified to read as noted in the markup as attached setting the tip rate C&D at $135.00; and

BE IT FURTHER RESOLVED, this amendment shall take effect on June 1, 2026.

	Ferndale, Monticello	Highland, Rockland, Mamakating, Western	Monticello
	Residential & Commercial		Collector Hauler
Municipal Solid Waste ($20 minimum for 292 lbs. or less) ($30 minimum for cu yd)	$160 /ton $85 per cubic yard	$185 /ton $85 per cubic yard	$150 /ton NA
C&D / Bulky Waste ($20 minimum for 267 lbs. or less) ($30 minimum for cu yd)	$160 /ton $85 per cubic yard	$185 /ton $85 per cubic yard	$135 /ton NA
Household Bagged Garbage 1 coupon per bag/can (up to 30 gallons)	5-Coupon book: $15 10- Coupon Book: $30	5-Coupon book: $15 10- Coupon Book: $30	NA NA
Single Stream Recycling	FREE (One 55-gallon drum or less)	FREE (One 55-gallon drum or less)	$125 per ton
Tires (with or without rims)	**4 tires or less:** 19" Rim or smaller: $5 per tire Over 19" rim: $30 per tire **5 or more**: $300 per ton	**4 tires or less:** 19" Rim or smaller: $5 per tire Over 19" rim: $30 per tire **5 or more**: $300 per ton	$300 per ton
CFC - Containing Appliances (refrigerators & freezers, air conditioners, dehumidifiers, etc)	$20	$20	$20
1 lb Propane tanks **20 lb Propane tanks**	Free $2	Free $2	Free $2
Permits	Free	Free	$150 plus $25/truck
Un-tarped Load fine	$10 (Less than 4 cubic yards) $100 (4 cubic yards or more)	$10 (Less than 4 cubic yards)	$10 (Less than 4 cubic yards) $100 (4 cubic yards or more)
Weight ticket service fee	$10	$10	$10

Reso Changes to C&D Only

	Ferndale, Monticello	Highland, Rockland, Mamakating, Western	Monticello
	Residential & Commercial		Collector Hauler
Municipal Solid Waste ($20 minimum for 292 lbs. or less) ($30 minimum for cu yd)	$137 /ton $60 per cubic yard	$137 /ton $60 per cubic yard	$137 /ton NA
C&D / Bulky Waste ($20 minimum for 296 lbs. or less) ($30 minimum for cu yd)	***is $150 as of 5/1/2026 $135 /ton $60 per cubic yard	$135 /ton $60 per cubic yard	$135 /ton NA
Household Bagged Garbage 1 coupon per bag/can (up to 30 gallons)	5-Coupon book: $15 10- Coupon Book: $30	5-Coupon book: $15 10- Coupon Book: $30	NA NA
Single Stream Recycling	FREE (One 55-gallon drum or less)	FREE (One 55-gallon drum or less)	$110 per ton
Tires (with or without rims)	**4 tires or less:** 19" Rim or smaller: $3 per tire Over 19" rim: $30 per tire **5 or more**: $300 per ton	**4 tires or less:** 19" Rim or smaller: $3 per tire Over 19" rim: $30 per tire **5 or more**: $300 per ton	$300 per ton
CFC - Containing Appliances (refrigerators & freezers, air conditioners, dehumidifiers, etc)	$15	$15	$15
1 lb Propane tanks **20 lb Propane tanks**	Free $2	Free $2	Free $2
Permits	Free	Free	$150 plus $25/truck
Un-tarped Load fine	$10 (Less than 4 cubic yards) $100 (4 cubic yards or more)	$10 (Less than 4 cubic yards)	$10 (Less than 4 cubic yards) $100 (4 cubic yards or more)
Weight ticket service fee	$10	$10	$10

100 North Street
Monticello, NY 12701

Sullivan County

Legislative Memorandum

File #: ID-8376 **Agenda Date:** 5/21/2026 **Agenda #:** 21.

Narrative of Resolution:
To Modify the 2026 Budget

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: Please see attached Budget Mods.

Are funds already budgeted? Choose an item.

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: Click or tap here to enter text.

Specify Compliance with Procurement Procedures:

RESOLUTION INTRODUCED BY MANAGEMENT & BUDGET COMMITTEE TO MODIFY THE 2026 BUDGET

WHEREAS, the County of Sullivan Budget requires modification,

NOW, THEREFORE, BE IT RESOLVED, that the attached budgetary transfers for 2026 be authorized.

April 30, 2026 Resolution Needed
Sullivan County Budget Modifications 2026

G/L Account	Revenue Increase	Revenue Decrease	Appropriation Increase	Appropriation Decrease
A-1165-40-4001 - CONTRACT AGENCIES			42,303	
A-1165-40-4001 - CONTRACT AGENCIES			28,841	
A-1165-40-4001 - CONTRACT AGENCIES			28,720	
A-1165-40-4001 - CONTRACT AGENCIES			54,768	
A-1165-43-4304 - COMPUTER MAINTENANCE/SERVICE FEES				1,116
A-1165-47-4792 - DEPT FORFEITURE PROCEEDS - COUNTY (*)			11,047	
A-1165-R4089-R167 - FED AID OTHR DEPARTMENTAL AID	54,768			
A-1165-R4089-R167 - FED AID OTHR DEPARTMENTAL AID	28,720			
A-1165-R4089-R167 - FED AID OTHR DEPARTMENTAL AID	28,841			
A-1165-R4089-R167 - FED AID OTHR DEPARTMENTAL AID	42,303			
A-1185-47-4719 - DEPT MORGUE FEES			10,000	
A-1340-47-4710 - DEPT DEPT MISC/OTHER			1,623	
A-1340-R2210-R134 - GEN SERV OTHR GOV CHARGBK - INTERDEPARTMNTL	1,623			
A-1620-23-R1710-R247 - PUBLIC WORKS CHARGE MISC FEE/REIMBURSMNT		1,763,486		
A-1620-24-R1289-R134 - GEN GOV DEPT INCOME CHARGBCK - INTERDEPARTMNTL	1,763,486			
A-1680-43-4302 - COMPUTER HARDWARE PURCHASES/LEASES			653	
A-1680-43-4304 - COMPUTER MAINTENANCE/SERVICE FEES			1,014	
A-1680-43-4304 - COMPUTER MAINTENANCE/SERVICE FEES			1,116	
A-1680-R1289-R247 - GEN GOV DEPT INCOME MISC FEE/REIMBURSMNT	1,667			
A-1989-99-47-4736 - DEPT CONTINGENT				10,000
A-3010-212-46-4612 - MISC SERV/EXP EMPL TRAINING			25,000	
A-3010-44-4406 - UTILITY WIRELESS COMMUNICATIONS			36,465	
A-3010-R3389-R338 - ST AID PUBLIC SAFETY OTHER	25,000			
A-3010-R4389-R338 - FED AID PUBLIC SAFETY OTHER	36,465			
A-3140-18-41-4105 - AUTO/TRAVEL REGISTRATION FEES (**)			180	
A-3140-18-42-4206 - OFFICE PUBLICATIONS (**)			1,472	
A-3140-18-43-4304 - COMPUTER MAINTENANCE/SERVICE FEES (**)			147	
A-3140-18-43-4304 - COMPUTER MAINTENANCE/SERVICE FEES (**)			180	
A-3140-18-45-4506 - SPEC DEPT SUPPLY PUBLIC SAFETY (**)			13,016	
A-3140-18-45-4507 - SPEC DEPT SUPPLY MEDICAL/CLINICAL (**)			890	
A-3140-18-46-4603 - MISC SERV/EXP EMPL UNIFORM ALLOWANCE (**)			9,527	
A-3140-18-47-4750 - DEPT CLIENT ELECTONIC MONITORING (**)			630	

G/L Account	Revenue Increase	Revenue Decrease	Appropriation Increase	Appropriation Decrease
A-6010-38-40-4013 - CONTRACT CONTRACT OTHER (***)			17,530	
A-6010-38-40-4013 - CONTRACT CONTRACT OTHER (***)			8,223	
A-6010-38-42-4201 - OFFICE ADVERTISING (***)			2,454	
A-6010-38-42-4201 - OFFICE ADVERTISING (***)			7,362	
A-6010-38-42-4203 - OFFICE OFFICE SUPPLIES			1,456	
A-6010-38-42-4207 - OFFICE FURNITURE			7,500	
A-6010-57-R4610-R228 - FED AID DFS ADMIN JOBS TITLE XX	8,956			
A-7110-230-40-4006 - CONTRACT ENGINEER/ARCHITECT/DESIGN SERV (****)			435	
A-8020-90-40-4006 - CONTRACT ENGINEER/ARCHITECT/DESIGN SERV (*****)			1,213	
A-8020-90-40-4013 - CONTRACT CONTRACT OTHER			32,279	
A-8020-90-R4089-R167 - FED AID OTHR DEPARTMENTAL AID	32,279			
A Fund Total	**2,024,108**	**1,763,486**	**346,044**	**11,116**

(*) To be funded from the DA County Drug Forfeiture Assigned Fund Balance
(**) To be funded from the Probation PTR Assigned Fund Balance
(***) To be funded from the Opioid Assigned Fund Balance
(****) To be funded from the Planning Programs Assigned Fund Balance
(*****) To be funded from the O&W Assigned Fund Balance

100 North Street
Monticello, NY 12701

Sullivan County

Legislative Memorandum

File #: ID-8324 **Agenda Date:** 5/21/2026 **Agenda #:** 22.

Narrative of Resolution:
Ratify a MOA with Teamsters Probation Unit

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: Click or tap here to enter text.

Are funds already budgeted? Choose an item.

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: Click or tap here to enter text.

Specify Compliance with Procurement Procedures:

RESOLUTION INTRODUCED BY THE EXECUTIVE COMMITTEE RATIFYING A MEMORANDUM OF AGREEMENT BETWEEN THE COUNTY OF SULLIVAN AND THE TEAMSTERS LOCAL 445, INTERNATIONAL BROTHERHOOD OF TEAMSTERS PROBATION UNIT AND AUTHORIZING THE COUNTY MANAGER TO EXECUTE SAID AGREEMENT

WHEREAS, the collective bargaining agreement between the County of Sullivan and the Teamsters Local 445, International brotherhood of Teamsters Probation Unit (hereinafter "Teamsters Probation Unit") expired on December 31, 2025;

WHEREAS, negotiations conducted pursuant to the provisions of Article 14 of the New York State Civil Service Law (Public Employees Fair Employment Act) have resulted in a Memorandum of Agreement for calendar year 2026 through 2029, attached hereto and made a part hereof; and

WHEREAS, the employees represented by Teamsters Probation Unit have voted and ratified the terms and conditions of employment, as set forth in the aforementioned Memorandum of Agreement.

NOW, THEREFORE, BE IT RESOLVED, that the terms and conditions of employment of employees represented by Teamsters Probation Unit, as set forth in the Memorandum of Agreement attached hereto and made a part hereof be and hereby are ratified, in recognition of the ratification by Teamsters Probation Unit; and

BE IT FUTHER RESOLVED, the County Manager is hereby authorized to execute an Agreement incorporating the terms and conditions of employment in accordance with the Memorandum of Agreement, said Collective Bargaining Agreement to be in such form as the County Attorney shall approve.

4/7/26

MEMORANDUM OF AGREEMENT

By and Between the

County of Sullivan
(hereinafter referred to as "County" or "Employer")

and the

Teamsters Local 445,
International Brotherhood of Teamsters
(Sullivan County Probation Department Unit)
(hereinafter referred to as the "Teamsters" or "Union")

WHEREAS, the County, and the Union are parties to a Collective Bargaining Agreement for the term January 1, 2021 through December 31, 2025; and

WHEREAS, the County and the Union have been engaged in collective bargaining, which has led to a mutual understanding between the County and the Union for the terms and conditions of employment for a Successor Agreement; and

WHEREAS, the County and the Union are desirous of reducing that mutual understanding to a written document.

NOW, THEREFORE, the County and the Union agree as follows:

1. All terms and conditions of the existing Collective Bargaining Agreement shall continue in full force and effect unless specifically modified by this Memorandum of Agreement and/or the terms of the expired Agreement.

2. This Memorandum of Agreement is subject to ratification by the membership of the Union and by the County Legislature of the County of Sullivan.

3. Amend **Section 302** to read as follows:

> 302. Effective January 1, 2026, the attached salary schedule shall be the new Appendix A to the Collective Bargaining Agreement for the period January 1, 2026 through December 31, 2029.

4. **Section 1201, at the County's option, the current Holiday Schedule may be replaced with the following:**

1201. The following days shall be allowed as days off with pay: New Year's Day, Dr. Martin Luther King Day, President's Day, Memorial Day, Juneteenth, Independence Day, Labor Day, Thanksgiving Day, the day after Thanksgiving Day, Christmas Day, Veteran's Day and Columbus Day.

In addition, employees will receive two (2) Floating Holidays per year which must be used prior to using vacation leave.

Whenever any holidays listed above fall on Saturday, the preceding Friday shall be observed as the holiday. Whenever any of the holidays listed above shall fall on a Sunday, the succeeding Monday shall be observed as the holiday. An employee must have worked his last scheduled work day before the holiday and the first scheduled work day after the holiday to receive compensation for the holiday, unless he/she was off because of illness, vacation, personal leave or any other reason which is acceptable to the Employer. Should the President of the United States or the Governor of New York State declare any day other than the above as a day of mourning, said day shall be honored by the County and applicable as paid leave to the employee covered by this Agreement. Should a holiday fall within an approved paid leave time, such holiday will be paid as a holiday and not charged to the employee's approved leave.

5. Amend **Section 401** by adding the following:

An employee may elect to take their paid lunch at anytime during the work day and in combination with the use of any accrued time, such as flex, personal, vacation, sick or compensatory time.

6. **Section 409.a)** shall be amended to read as follows:

409.

a) When an employee is working in the office or on a regularly scheduled remote work day, and the need arises for personal reasons to flex the hours in their work day, they may, provided they receive prior approval via text, email or verbally from the Supervisor, Deputy Director or Director. The amount of time flexed in any given week may not exceed two hours. If approval is given via text or verbally, the employee will follow up with an email to the individual who granted the approval and the timekeeper will be copied so there is a written record of the request and approval. Payback of the time flexed can be made in the same week, in the office, in individual or multiple increments of 15 minutes. On a regularly scheduled remote work day, the hours worked cannot exceed eight.

7. **Section 708** shall be amended by deleting the last sentence and adding the following:

The County shall provide yearly training in the use of the TASER Conducted Energy Weapon.

8. **Section 710** shall be amended by removing "Polo" style shirts and adding "solid color pants."

9. **Section 1003** shall be amended to read as follows:

1003. The County shall provide, as outlined in the amended Code of the County regarding a centralized motor pool vehicles as necessary at the Monticello Complex. Employees shall not be required to utilize their personal vehicles to transport clients.

10. **Section 1304** shall be amended by adding the following:

In addition to the above, vacation time may be taken in 15-minute increments or multiples thereof subject to department head approval.

11. **Article XIV – Bereavement Leave, Section 1401,** shall be amended to include step-children and step-parent.

12. **Section 1805.b.vi.,** shall be amended to read as follows:

vi. Effective January 1, 2026, an employee who is entitled to individual coverage who opts out of that coverage shall be paid $6,000.00. An employee who is entitled to family coverage but opts only to take individual coverage shall be entitled to an opt out payment of $6,000.00. An employee who is entitled to family coverage who opts out completely will be entitled to an annual payment of $12,000.00. No employee shall be eligible to receive such payment unless the employee shall have presented proof to the Director of Risk Management that such employee and such employee's eligible dependents are covered by a comparable plan of medical and health insurance benefits for the entire year that such employee elected not to be covered by the plan of medical and health insurance benefits provided by the employer. An employee who receives coverage under a family plan from a spouse who is employed by the county shall still be eligible to receive the "opt out" payment should the spouse choose to pay the premium contribution as per their date of hire, regardless of their bargaining unit.

13. Add a new Section to be **Section 1327** which shall read as follows:

General

1327. The County has a leave donation policy for eligible employees who are severely ill and who are quickly depleting their leave credits. In addition to the parameters of leave donations contained in the policy, employees are allowed to donate annually a total of up to five (5) days of combined personal and sick leave days to eligible employees. This 5-day limit is an annual total limit which an employee may donate regardless of the number of employees who may be eligible.

14. Add a new Section to be **Section 311** which shall read as follows:

311. The Employer shall provide stipends in addition to regular compensation for employees who perform the following services in the following amounts:

Defensive Tactics Instructor - $1,000 annually
Firearms Instructor - $1,000 annually
Taser Instructor - $1,000 annually
Chemical Agent Instructor - $1,000 annually
Department Armor - $500 annually

An employee may only receive one (1) of the above stipends per year. The number of individuals who shall receive the stipends shall be determined annually by the Probation Director, subject to the approval of the County Manager. The annual stipends shall be paid only to those individuals approved to receive such stipend during the given year by the Probation Director and the County Manager. The annual stipends shall be paid only to those individuals approved to receive such stipends during the given year. In the event an employee receiving a stipend discontinues performing the duties that make them eligible for a stipend, the employee will no longer be eligible for the remainder of the stipend.

15. In the event that the County Legislature authorizes participation in the New York State Paid Family Leave Program, the benefit will be available to members of this bargaining unit.

IN WITNESS WHEREOF, the parties have hereunto set their hands and seals this _____ day of April, 2026.

COUNTY OF SULLIVAN

By: _____
Joshua Potosek, County Manager

By: _____
Michelle Bowers, Deputy County Manager

By: _____
Julie Diescher, HR Commissioner

TEAMSTERS LOCAL 445, INTERNATIONAL BROTHERHOOD OF TEAMSTERS (SULLIVAN COUNTY PROBATION DEPARTMENT UNIT)

By: _____
Ray Stanishia, Business Agent

APPENDIX A

Probation Assistant	Entry	Full
Jan. 1, 2025	46,275	48,710
Jan. 1, 2026	47,662	50,171
Jan. 1, 2027	49,092	51,676
Jan. 1, 2028	50,565	53,226
Jan. 1, 2029	52,082	54,823

Probation Officer Trainee	Entry	Full
Jan. 1 2025	62,954	66,267
Jan. 1, 2026	64,842	68,255
Jan. 1, 2027	66,788	70,303
Jan. 1, 2028	68,791	72,412
Jan. 1, 2029	70,855	74,584

Probation Officer	Entry	Full	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8	Step 9	Step 10	Step 15	Step 20
Jan. 1 2025	67,351	70,896	71,790	72,686	73,580	74,474	75,369	76,263	77,158	78,054	78,949	79,843		
Jan. 1, 2026	69,372	73,023	74,201	75,382	76,560	77,738	78,918	80,096	81,275	82,456	83,635	84,813	85,586	86,358
Jan. 1, 2027	71,453	75,214	76,427	77,643	78,857	80,070	81,286	82,499	83,713	84,930	86,144	87,357	88,154	88,949
Jan. 1, 2028	73,597	77,470	78,720	79,972	81,223	82,472	83,725	84,974	86,224	87,478	88,728	89,978	90,799	91,617
Jan. 1, 2029	75,804	79,794	81,082	82,371	83,660	84,946	86,237	87,523	88,811	90,102	91,390	92,677	93,523	94,366

Senior Probation Officer	Entry	Full	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8	Step 9	Step 10	Step 15	Step 20
Jan. 1 2025	71,748	75,524	76,417	77,314	78,208	79,102	79,997	80,892	81,787	82,681	83,574	84,470		
Jan. 1, 2026	73,901	77,790	78,967	80,148	81,327	82,505	83,684	84,864	86,043	87,221	88,399	89,579	90,352	91,124
Jan. 1, 2027	76,118	80,124	81,336	82,552	83,767	84,980	86,195	87,410	88,624	89,838	91,051	92,266	93,063	93,858
Jan. 1, 2028	78,402	82,528	83,776	85,029	86,280	87,529	88,781	90,032	91,283	92,533	93,783	95,034	95,855	96,674
Jan. 1, 2029	80,754	85,004	86,289	87,580	88,868	90,155	91,444	92,733	94,021	95,309	96,596	97,885	98,731	99,574

Probation Supervisor	Entry	Full	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8	Step 9	Step 10	Step 15	Step 20
Jan. 1 2025	83,840	88,253	89,147	90,041	90,936	91,832	92,726	93,620	94,514	95,409	96,305	97,198		
Jan. 1, 2026	86,356	90,901	92,079	93,257	94,437	95,617	96,795	97,974	99,152	100,331	101,512	102,689	103,461	104,234
Jan. 1, 2027	88,947	93,628	94,841	96,055	97,270	98,486	99,699	100,913	102,127	103,341	104,557	105,770	106,565	107,361
Jan. 1, 2028	91,615	96,437	97,686	98,937	100,188	101,441	102,690	103,940	105,191	106,441	107,694	108,943	109,762	110,582
Jan. 1, 2029	94,364	99,330	100,617	101,905	103,194	104,484	105,771	107,058	108,347	109,634	110,925	112,211	113,055	113,899

NOTE: Probation Officer Titles that currently have salaries over the salary schedule will receive any increases based on their current salary and not the schedule; any employee being promoted or demoted will go to their respective step on the salary schedule. Step Increases are given on January 1 following the year of completion.

File #: ID-8335 **Agenda Date:** 5/21/2026 **Agenda #:** 23.

Narrative of Resolution:
Set a public hearing 6/18/26 at 8:55am to Override the NYS Property Tax Cap for 2027

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: N/A

Are funds already budgeted? Choose an item.

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: Click or tap here to enter text.

Specify Compliance with Procurement Procedures: N/A

RESOLUTION INTRODUCED BY EXECUTIVE COMMITTEE TO SET A PUBLIC HEARING FOR A PROPOSED LOCAL LAW ENTITLED LOCAL LAW TO EXCEED THE NEW YORK STATE PROPERTY TAX CAP FOR 2027

WHEREAS, there has been introduced and presented at a meeting of the Sullivan County Legislature held on May 21, 2026 a proposed local Law entitled "A Local Law To Exceed the New York State Property Tax Cap for 2027".

NOW, THEREFORE BE IT RESOLVED, that a public hearing be held on said proposed local law by the Sullivan County Legislature on June 18, 2026 at 8:55a.m. in the Legislative Hearing Room, County Government Center, Monticello, New York and at least six (6) days' notice of the public hearing be given to the Clerk of the Sullivan County Legislature by due posting thereof on the bulletin board of the County of Sullivan and by publishing such notice at least once in the official newspapers of the County.

COUNTY OF SULLIVAN

NOTICE OF PUBLIC HEARING

NOTICE IS HERE BY GIVEN that there has been duly presented at a meeting of the Legislature of the County of Sullivan, New York, held on May 21, 2026, a proposed Local Law entitled "A Local Law to exceed the New York State property Tax Cap for 2027".

NOTICE IS FURTHER GIVEN that the Legislature of the County of Sullivan will conduct a public hearing on the aforesaid proposed Local Law at the Legislature's Hearing Room, County Government Center, Monticello, New York 12701 on June 18, 2026 at 8:55a.m. at which time all persons interested will be heard.

DATED: May 21, 2026

ANNMARIE MARTIN
Clerk of the Legislature
County of Sullivan, New York

A Local Law Authorizing the Sullivan County Legislature to Override the New York State Real Property Tax Cap

BACKGROUND

On June 24, 2011 the New York Real Property "Tax Cap" Chapter 97 "Part A" of the Laws of New York 2011, was signed into law. The aforesaid "Tax Cap" was incorporated as an amendment to the General Municipal Law as Section 3-c thereof, and was made applicable to counties.

INTENT

The Sullivan County Legislature in anticipation that it may be required to adopt a budget which imposes a tax levy increase greater than the limit set forth in the General Municipal Law Section 3-c for the fiscal year 2027 desires to enact a Local Law granting it such authority.

AUTHORITY

General Municipal Law Section 3-c(5) authorizes counties to enact a Local Law enabling them to exceed the Tax Cap in the coming fiscal year.

> A Local government may adopt a budget that requires a tax levy that is greater than the tax levy limit for the coming fiscal year, not including any levy necessary to support the expenditures pursuant to the subparagraphs (i) through (iv) of paragraph g of subdivision two of this section, only if the governing body of such local government first enacts, by a vote of sixty percent of the total voting power of such body, a local law to override such limit for such coming fiscal year only…"

BE IT ENACTED by the Legislature of the County of Sullivan, as follows:

SECTION 1. Pursuant to authority granted to the Sullivan County Legislature by Municipal Law Section 3-c(5) the Sullivan County Legislature is hereby authorized to adopt a budget which exceeds the "Tax Levy Limit" for fiscal year 2027.

SECTION 2. This Local Law shall become effective upon filing with the Secretary of State.

File #: ID-8343 **Agenda Date:** 5/21/2026 **Agenda #:** 24.

Narrative of Resolution:
Establish a Standard Work Day for an Elected Official

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $0

Are funds already budgeted? Choose an item.

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: Click or tap here to enter text.

Specify Compliance with Procurement Procedures:

RESOLUTION INTRODUCED BY EXECUTIVE COMMITTEE TO ESTABLISH A STANDARD WORK DAY FOR ELECTED AND APPOINTED OFFICIALS

WHEREAS, effective August 12, 2009, New York State adopted a new regulation 315.4 for additional reporting requirements for elected or appointed officials that more clearly defines the process for reporting time worked for those officials who are members of the New York State Retirement System, and

WHEREAS, one (1) three month record of work activities were submitted to the Clerk of the Legislature by the elected official that does not maintain a daily record of actual time worked.

NOW THEREFORE BE IT RESOLVED, that the Sullivan County Legislature hereby establishes the following as a standard work day for elected and appointed officials and will report the following days worked to the New York State and Local Employees' Retirement System based on the record of activities maintained and submitted by these official(s) to the Clerk of the Legislature.

BE IT FURTHER RESOLVED, that the Sullivan County Legislature does hereby attest that the above elected official has submitted a three-month log of activities and such is on file with the Clerk to the Legislature.

Kathleen Lara, County Treasurer

Term: 1/1/2026-12/31/2029

Standard Work day: 7 hours

Does not participate in Employers Time Keeping System

Days per month based on Record of Activities: 25.45

Filed a 90 day log

100 North Street
Monticello, NY 12701

Sullivan County

Legislative Memorandum

File #: ID-8347 **Agenda Date:** 5/21/2026 **Agenda #:** 25.

Narrative of Resolution:
The Legislative Discretionary Funding program is designed to assist Sullivan County and County-oriented entities with achieving such goals as public safety, public health, youth services, community development, and economic development

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $30,774

Are funds already budgeted? Yes

Specify Compliance with Procurement Procedures: N/A

RESOLUTION INTRODUCED BY THE EXECUTIVE COMMITTEE TO AUTHORIZE FUNDING THROUGH THE LEGISLATIVE DISCRETIONARY FUNDING PROGRAM

WHEREAS, the Sullivan County Legislature adopted a Legislative Discretionary Contract Funding Program pursuant to Resolution No. 327-16; and

WHEREAS, the program is designed to assist Sullivan County and County-oriented entities with achieving such goals as public safety, public health, youth services, community development, and economic development; and

WHEREAS, the program review took place during the 2026 Budget process and the Legislature had an opportunity to assess the applications submitted;

NOW, THEREFORE, BE IT RESOLVED, that the Sullivan County Legislature approves the projects listed in the below "Schedule A" and the disbursement of the associated funds, and

BE IT FURTHER RESOLVED, that the Sullivan County Legislature authorizes the County Manager to enter into contracts with these award recipients for the contract period of January 1, 2026 through December 31, 2026 for said services as submitted in their application; and

BE IT FURTHER RESOLVED, that the below organizations may request that the County advance these funds with the acknowledgment that there shall be the appropriate proof submitted to the Management and Budget Division at the completion of their purchase or their program no later than December 31, 2026; and

BE IT FURTHER RESOLVED, said contracts to be in a form approved by the County Attorney.

"Schedule A"

2026 Legislative Discretionary Contract Funding

Applicant	**Award Recommendation**
Eldred Little League	$1,474 (Legislator District 2- Additional funding)
People Patch Foundation, Inc.	$7,000 (Legislator District 8)
STEAM Fund at CFOS	$2,500 (Legislator District 8) $1,800 (District 3 Legislator), $500 (District 2 Legislator)
Hurleyville Performing Arts Centre, Inc.	$500 (Legislator District 8)
The Civic Association of Smallwood NY, Inc.	$6,000 (Legislator District 1)
Kauneonga Lake Fire Department	$2,000 (Legislator District 1)

Sullivan County Youth Baseball & Softball League-Sullivan West Cal Ripken	$4,000 (Legislator District 5)
Sullivan Health Access, Inc.	$5,000 (Legislator District 5)

File #: ID-8383 **Agenda Date:** 5/21/2026 **Agenda #:** 26.

Narrative of Resolution:
Amend Resolution No, 138-26 correcting the amount

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: N/A

Are funds already budgeted? Choose an item.

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: Click or tap here to enter text.

Specify Compliance with Procurement Procedures:

RESOLUTION INTRODUCED BY THE EXECUTIVE COMMITTEE TO AMEND THE AMOUNT AUTHORIZED BY RESOLUTION 138-26 FOR THE 26-27 GOVERNOR'S TRAFFIC SAFETY COMMITTEE APPLICATION FOR THE CHILD PASSENGER SAFETY PROGRAM

WHEREAS, Resolution 138-26 authorized an application for the 26-27 Governor's Traffic Safety Committee: Child Passenger Safety Program funding in the amount of $15,000**;** and

WHEREAS, the application that was submitted requested $29,099 in funding; and

WHEREAS, all grant applications that are submitted by the County of Sullivan must follow the correct legislative procedure ensuring funding amounts applied for are equal to or less than the amount authorized by resolution; and

WHEREAS, the Governor's Traffic Safety Committee grant requires no matching funds resulting in the need to authorize only a greater award amount;

NOW, THEREFORE, BE IT RESOLVED, that the Sullivan County Legislature hereby amends Resolution 138-26 to authorize the application to the Governor's Traffic Safety Committee: Child Passenger Safety Program in the amount of $29,099; and

BE IT FURTHER RESOLVED, that the Sullivan County Legislature hereby authorizes the Chairman of the

County Legislature (*as required by the funding source*) to accept the award, and enter into an award agreement or contract to administer the funding secured, in such form as the County Attorney shall approve; and

BE IT FURTHER RESOLVED, that should the Governor's Traffic Safety Committee funding be terminated, the County shall not be obligated to continue any action undertaken by the use of this funding.

100 North Street
Monticello, NY 12701

Sullivan County

Legislative Memorandum

File #: ID-8377 **Agenda Date:** 5/21/2026 **Agenda #:** 27.

Narrative of Resolution:
Authorize three (3) 2027 GTSC (Governor's Traffic Safety Committee) Grant Applications

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $0

Are funds already budgeted? Choose an item.

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: Click or tap here to enter text.

Specify Compliance with Procurement Procedures:

RESOLUTION INTRODUCED BY THE EXECUTIVE COMMITTEE FOR THE SULLIVAN COUNTY LEGISLATURE TO ACT IN ITS CAPACITY AS LOCAL BOARD FOR THE GOVERNOR'S TRAFFIC SAFETY COMMITTEE (GTSC) TO AUTHORIZE APPROVAL OF THREE (3) 2027 GTSC GRANT APPLICATIONS

WHEREAS, each County's local Traffic Safety Board is responsible for approving all applications submitted to the New York State Governor's Traffic Safety Committee within each respective County; and

WHEREAS, the Governor's Traffic Safety Committee is seeking the approval of these three (3) applications, and

WHEREAS, the Sullivan County Traffic Safety Board hereby approves the following grant applications for FY 2027:

- County of Sullivan Department of Public Health Child Passenger Safety Grant Application requesting $29,099
- County of Sullivan Sheriff's Office Police Traffic Services Grant Application requesting $9,960
- Town of Fallsburg Police Department Police Traffic Services Grant Application requesting $5,550

NOW, THEREFORE, BE IT RESOLVED, that the Sullivan County Traffic Safety Board hereby approves the three (3) above named FY2-27 grant applications.

File #: ID-8381 **Agenda Date:** 5/21/2026 **Agenda #:** 28.

Narrative of Resolution:
TO APPLY FOR AND ACCEPT THE COMBINED FY2025 & FY2026 STATEWIDE INTEROPERABLE COMMUNICATIONS (SICG) FORMULA-BASED GRANT PROGRAM
If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $1,109,208.00

Are funds already budgeted? No

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: A-3020-44-4406

Specify Compliance with Procurement Procedures: N/A

RESOLUTION INTRODUCED BY THE EXECUTIVE COMMITTEE TO AUTHORIZE THE COUNTY MANAGER TO APPLY FOR AND ACCEPT THE COMBINED FY2025 & FY2026 STATEWIDE INTEROPERABLE COMMUNICATIONS (SICG) FORMULA-BASED GRANT PROGRAM ADMINISTERED BY THE NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES (NYS DHSES)

WHEREAS, the New York State Division of Homeland Security and Emergency Services (NYS DHSES) provides funds to support efforts of emergency management/homeland security; and

WHEREAS, the NYS DHSES - Office of Interoperable and Emergency Communications (OIEC), is administering the combined FY2025 & FY2026 Statewide Interoperable Communications Formula-Based Grant (SICG) program to provide reimbursement for costs associated with enhancing emergency response; improving capability, governance structures, operating procedures, infrastructure development; and addressing SAFECOM guidance; and

WHEREAS, the Sullivan County Division of Public Safety has been deemed eligible for the funding in the amount of $1,109,208.00 to support the improvement of public safety communications and PSAP operations; and

WHEREAS, the Sullivan County Division of Public Safety - E911 Communications Department must submit an application in order to receive said funds and wishes to file an application with the grant program; and

WHEREAS, Sullivan County is not required to provide a local cash or in-kind match in support of the SICG program.

NOW THEREFORE BE IT RESOLVED, that the Sullivan County Division of Public Safety - E911 Communications Department is hereby authorized to prepare an application for funding under the NYS DHSES OIEC SICFBG program.

BE IT FURTHER RESOLVED, that the Sullivan County Legislature hereby authorizes the County Manager, Chairman of the County Legislature, and / or their authorized representative (as required by the funding source) to execute any and all necessary documents to submit the combined FY2025 & FY2026 NYS DHSES OIEC SICFBG program application for funding; and

BE IT FURTHER RESOLVED, that the Sullivan County Legislature hereby authorizes the County Manager and / or Chairman of the County Legislature (as required by the funding source) to accept the award, and enter into an award agreement or contract to administer the funding secured, in such form as the County Attorney shall approve; and

BE IT FURTHER RESOLVED, that if awarded DHSES grant funding, the Sullivan County Division of Public Safety - E911 Communications Department, shall administer the funds and grant program; and

BE IT FURTHER RESOLVED, that should the DHSES grant funding program be terminated, the County shall not be obligated to continue any action undertaken by the use of this funding.

File #: ID-8382 **Agenda Date:** 5/21/2026 **Agenda #:** 29.

Narrative of Resolution:
TO AUTHORIZE AN ADDITIONAL SERVICES AGREEMENT WITH JAMES McGUINNESS & ASSOCIATES, INC. FOR eSTACs IMPLEMENTATION AND SUPPORT SERVICES FOR PUBLIC HEALTH SERVICES

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $56,000.00

Are funds already budgeted? Yes

If 'Yes,' specify appropriation code(s): A-1680-43-4304

If 'No,' specify proposed source of funds: N/A

Specify Compliance with Procurement Procedures: Quote received from long-standing solution provider to PHS for the additional eSTAC (electronic System to Track and Account for Children) module.

RESOLUTION INTRODUCED BY THE EXECUTIVE COMMITTEE TO AUTHORIZE AN ADDITIONAL SERVICES AGREEMENT WITH JAMES McGUINNESS & ASSOCIATES, INC. FOR eSTACs IMPLEMENTATION AND SUPPORT SERVICES FOR PUBLIC HEALTH SERVICES

WHEREAS, by Resolution No. 107-26, the Sullivan County Legislature authorized a one (1) year agreement with James McGuinness & Associates, Inc. for software and related services utilized by Sullivan County Public Health Services' Early Intervention Preschool Handicapped Program; and

WHEREAS, Sullivan County Public Health Services has identified a need for additional electronic System to Track and Account for Children ("eSTAC") functionality and integration services to improve the management, exchange, and processing of preschool-related student, evaluation, and service data between school districts and the County's preschool software system; and

WHEREAS, James McGuinness & Associates, Inc. has submitted a proposal to provide eSTACs implementation services, including system configuration, integration, setup, support, and maintenance services for Sullivan County Public Health Services; and

WHEREAS, the proposed additional services include a one-time implementation/setup fee in the amount of $50,000.00 and ongoing support and maintenance services in the amount of $1,000.00 per month; and

WHEREAS, Sullivan County Public Health Services wishes to proceed with implementation of the eSTACs platform beginning July 1, 2026, with said additional services to co-term with the existing annual agreement on December 31, 2026;

NOW, THEREFORE, BE IT RESOLVED, that the County Manager is hereby authorized to enter into an additional services agreement and/or amendment to the existing agreement with James McGuinness & Associates, Inc. for eSTACs implementation, support, and maintenance services for Sullivan County Public Health Services for the period July 1, 2026 through December 31, 2026; and

BE IT FURTHER RESOLVED, that said agreement and/or amendment shall authorize:

- a one-time implementation and setup fee in an amount not to exceed $50,000.00; and
- support and maintenance fees in an amount not to exceed $1,000.00 per month for the remainder of calendar year 2026; and

BE IT FURTHER RESOLVED, that the total amount authorized pursuant to this resolution shall not exceed $56,000.00; and

BE IT FURTHER RESOLVED, that the form of said agreement and/or amendment shall be approved by the County Attorney.

100 North Street
Monticello, NY 12701

Sullivan County

Legislative Memorandum

File #: ID-8387 **Agenda Date:** 5/21/2026 **Agenda #:** 30.

Narrative of Resolution:
Authorize contract with Sterling Environmental Engineering, P.C. to provide technical consulting with review of the Town Line Solar and Battery Storage Project

If Resolution requires expenditure of County Funds, provide the following information:

Amount to be authorized by Resolution: $98,200 plus incidental expenses

Are funds already budgeted? No

If 'Yes,' specify appropriation code(s): Click or tap here to enter text.

If 'No,' specify proposed source of funds: No County Money

Specify Compliance with Procurement Procedures:

RESOLUTION INTRODUCED BY THE EXECUTIVE COMMITTEE TO AUTHORIZE THE AWARD AND EXECUTION OF A CONTRACT WITH STERLING ENVIRONMENTAL ENGINEERING, P.C. TO PROVIDE INDEPENDENT TECHNICAL CONSULTING SERVICES IN CONNECTION WITH REVIEW OF THE TOWN LINE SOLAR AND BATTERY STORAGE PROJECT

WHEREAS, Sullivan County ("County") has entered into a memorandum of understanding with the Town of Forestburgh and the Town of Thompson (the "Towns") to jointly engage legal counsel and environmental/planning consultants to assist with a coordinated review of the Town Line Solar Project ("Project"); and

WHEREAS, the Project will be subject to review by the New York State Office of Renewable Energy Siting ("ORES") pursuant to Executive Law Section 94-c and its implementing regulations; and

WHEREAS, ORES regulations provide for the availability of local agency account ("Intervenor") funds to assist municipalities and local parties in participating in the permitting process; and

WHEREAS, the County issued a Request for Proposals, R-26-18, to retain qualified independent technical consultants to assist in reviewing the Project; and

WHEREAS, proposals received in response to R-26-18 have been reviewed by the County and the Towns, and the municipalities agree that Sterling Environmental Engineering, P.C. located at 24 Wade Road Latham, NY 12110, is the best qualified firm to provide the services required; and

WHEREAS, the total estimated cost of these services is $98,200, plus incidental expenses, as detailed in the attached fee schedule; and

WHEREAS, the cost of the services will be covered by the aforementioned intervenor funds made available as a requirement of the permitting process set forth by ORES, and neither the County nor the Towns shall be obligated to pay expenses beyond those fully covered by intervenor funds unless appropriate authorizations are secured from each municipality's governing body.

NOW, THEREFORE, BE IT RESOLVED, that the Sullivan County Legislature authorizes the County Manager to execute an agreement with Sterling Environmental Engineering, P.C., to provide independent technical consulting services in connection with a coordinated review of the Town Line Solar and Battery Storage Project, in such form as the County Attorney shall approve, in an amount not to exceed $98,200 plus incidental expenses.

RFP: #R-26-18
Independent Technical Consulting Services
Review of the Town Line Solar and Battery Storage Project

FEE PROPOSAL

Based upon Sterling Environmental Engineering, P.C.'s experience in the review and independent evaluation of large scale renewable energy projects, we provide the following estimate of labor and expenses. This estimate is made based on the project information provided in the RFP, prior to submission of the application by the Project Sponsor. Upon an initial review of the application documents, we anticipate assisting the County and Towns in applying for LAA funding. The budgeted level of effort for each discipline may be modified to allocate resources for the most meaningful review.

Task	Budget Total
Discipline A: Hydrology & Floodplain Engineering	
Principal Engineer	$1,200
Senior Engineer	$4,000
CAD/GIS Scientist	$8,000
Support Staff	$1,000
CAD/GIS Software & Expenses	$900
TOTAL DISCIPLINE A:	**$15,100**
Discipline B: Wetlands and Aquatic Ecology	
Principal Engineer	$600
Senior Engineer	$1,800
Wetland Scientist	$5,000
Environmental Analyst	$3,000
CAD/GIS Scientist	$1,500
CAD/GIS Software & Expenses	$900
TOTAL DISCIPLINE B:	**$12,800**
Discipline C: Wildlife Biology and Habitat Assessment	
To be subcontracted to qualified expert.	$8,000
TOTAL DISCIPLINE C:	**$8,000**
Discipline D: Forestry and Arborist Services	
To be subcontracted to qualified arborist.	$6,000
TOTAL DISCIPLINE D:	**$6,000**
Discipline E: Civil and Geotechnical Engineering	
Principal Engineer	$1,200
Senior Engineer	$5,000
CAD/GIS Engineer	$8,000
Engineering Technician	$4,000
CAD/GIS Software & Expenses	$1,200
TOTAL DISCIPLINE E:	**$19,400**

Discipline F: Visual Impact Analysis / Landscape Architecture	
Principal Engineer	$600
Senior Engineer	$2,500
CAD/GIS Engineer	$3,000
Landscape Architect (TBD) – Budget allocated.	$4,000
CAD/GIS Software & Expenses	$900
TOTAL DISCIPLINE F:	**$11,000**
Discipline G: Acoustical Engineering / Noise Analysis	
Principal Engineer	$1,200
Senior Engineer	$3,600
CAD/GIS Engineer	$4,000
Engineering Technician	$3,000
EM/RF Specialist Subcontractor (TBD) – Budget allocated.	$3,000
CAD/GIS Software & Expenses	$1,100
TOTAL DISCIPLINE G:	**$15,900**
Discipline H: Real Estate Economics and Property Value Analysis	
To be subcontracted to a qualified consultant.	$10,000
TOTAL DISCIPLINE H:	**$10,000**

Summary	Sterling Budgeted Effort	Subcontractor Budget
Discipline A: Hydrology & Floodplain Engineering	$15,100	
Discipline B: Wetlands and Aquatic Ecology	$12,800	
Discipline C: Wildlife Biology and Habitat Assessment		$8,000
Discipline D: Forestry and Arborist Services		$6,000
Discipline E: Civil and Geotechnical Engineering	$19,400	
Discipline F: Visual Impact Analysis / Landscape Architecture	$7,000	$4,000
Discipline G: Acoustical Engineering / Noise Analysis	$15,900	
Discipline H: Real Estate Economics and Property Value Analysis		$10,000
TOTAL:	**$70,200**	**$28,000**

STERLING's Standard Billing Rates is attached.

Sterling Environmental Engineering, P.C.

STANDARD BILLING RATES
(Effective January 2026)

Position	**Hourly Rate**
Chief Engineer / Vice President	$297
Senior Engineer / President	$195
Senior Engineer/Geologist	$180 – $225
Engineer/Geologist Project Manager	$115 – $180
Engineer/Geologist	$90 – $115
Environmental Scientist	$85 – $105
Environmental/Field Technician	$65 – $95
Operations Manager	$75 – $100
Clerical Services/Interns	$50 – $75

NOTE: Labor rates are subject to periodic adjustment.

"Serving our clients and the environment since 1993"

24 Wade Road ♦ Latham, New York 12110 ♦ Tel: 518-456-4900 ♦ Fax: 518-456-3532
E-mail: sterling@sterlingenvironmental.com ♦ Website: www.sterlingenvironmental.com

EXPENSES:

Expenses are itemized and invoiced at cost plus 15%.

Third Party Services	**Cost**
Subcontractors/Subconsultants (Laboratory, Drillers, etc)	@ Cost
Fieldwork	
Equipment Rental & Supplies	@ Cost
Level C PPE (e.g., Respirators)	Per quote
Level D PPE	$20/Person/Day
Field Truck	$100/Day
Meetings / Travel	
Expert Testimony	Per quote
Vehicle Mileage	IRS Reimbursement Rate
Travel (air, train, etc.), tolls, parking	@ Cost
Lodging / Meals	@ Cost
Telephone/Conference Line	@ Cost
Production	**Cost**
Black & White Photocopies	
8-1/2 x 11	$0.15/page
11 x 17	$0.25/page
Color Photocopies	
8-1/2 x 11	$0.75/page
11 x 17	$1.00/page
Plotter Prints:	
Black & White Engineer Drawings	$5.00/sheet
Color Engineer Drawings	$10.00/sheet
CADD/GIS/Other Engineering Software	$30/hour
Binders	@ Cost
Postage	@ Cost

NOTE: Expense rates are subject to periodic adjustment.