RESOLUTION NO. 439 – EXHIBIT A

ULSTER COUNTY, NY

Department of Information Services
25 South Manor Avenue
Kingston, NY 12401

Information Technology Policy	**Policy No:** UCIS-P0125-001
Information Security	**Updated:** 7/30/2025
	Issued By: Ulster County Information Services **Owner:** Information Security Officer

1.0 Purpose and Benefits

This policy defines the mandatory minimum information security requirements for all “County Entities”, as defined in Section 3.0 of this policy. A County Entity may, based on its individual business needs and specific legal, state and federal requirements, exceed the security requirements put forth in this policy, but must, at a minimum, achieve the security levels required by this policy.

This policy acts as an umbrella document to all other Ulster County Information Services (“UCIS”) security policies and associated standards. This policy defines the responsibility of all CEs to:

- Protect and maintain the Confidentiality, Integrity, and Availability of information and related infrastructure assets;
- Manage the risk of security exposure or compromise;
- Ensure a secure and stable information technology (IT) environment;
- Identify and respond to events involving information asset misuse, loss, or unauthorized disclosure;
- Monitor systems for anomalies that might indicate compromise; and
- Promote and increase the awareness of information security.

Failure to secure and protect the Confidentiality, Integrity, and Availability of information assets in today’s highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions, and vital government functions; compromise data; and result in legal and regulatory non-compliance.

The Policy aims to:

1. Establish an evolutionary, risk-managed Information Security program that defends against internal and external threats.
2. Establish a management structure that addresses the County's Information Security operations, and require that all Users of County Information Systems:
    a. Are knowledgeable of acceptable County Information System usage;
    b. understand their Information Security responsibilities;
    c. are held accountable for their actions.

Conflicting provisions contained in collective bargaining agreements, to the extent required by law, shall supersede this policy. Where collective bargaining agreements are silent, this Policy shall be applied.

In the event that any provision of this policy or application thereof shall be held invalid, this act shall not be construed to affect the validity of any other provision, or application thereof of this policy.

2.0 Authority

The Ulster County Legislature via Resolution #XXX has approved the adoption of this policy.

Section A15-1 of the Administrative Code provides that the Director of Information Services shall have the charge and duty of performing the following functions as the County Executive may direct, including:

a) Oversee and supervise the processing of information and data within County government;
b) develop programs designed to provide accurate, sufficient, and timely information for decision-making by all units of County government;
c) coordinate the organization, maintenance and use of equipment capable of providing information relating to the functions of County government;
d) direct the administrative activities of the department.

3.0 Scope

,

This policy applies to all “County Entities”, including employees, volunteers, temporary staff as well as third parties (such as other local governments/agencies, consultants, vendors, and contractors), that use or access any County IT resource for which Ulster County Information Services (UCIS) has administrative responsibility, including systems managed or hosted by third parties on behalf of the UCIS. This policy applies to users of any system’s information or physical infrastructure regardless of its form or format, created or used to support CEs. It is the user’s responsibility to read and understand this policy and to conduct their activities in accordance with its terms

This policy addresses all information, regardless of the form or format, which is created or used in support of business activities of County Entities.

4.0 Information Statement

4.1 Organizational Security

1. Information security requires both an information risk management function (including cyber-related risk management) and an information technology security function. Depending on the structure of the CE, an individual or group can serve in both roles, or a separate individual or group can be designated for each role. It is recommended that these functions be performed by a high-level executive or a group that includes high-level executives.

    a. Each County Entity must designate an individual or group to be responsible for the information security risk management function. For purposes of this policy, the Department of Information Services shall serve as the information security risk management for county departments. Other entities (such as local governments/agencies, consultants, vendors, contractors, including their employees and subcontractors), that use or access any County IT resource for which the UCIS has administrative responsibility must designate an individual or group to be responsible for the information security management function. This policy will refer to the individual or group so designated as the Cyber Risk Coordinator (CRC) (*see* Appendix A for a more detailed description of the role). The CRC is responsible for ensuring that:

        i. Risk considerations for information assets and systems, including authorization decisions, are evaluated from the county entity's perspective in relation to its strategic goals and core mission.

        ii. The management of information assets, information system-related security risks, and other cyber-security risks is consistent across the County Entity, reflects the risk tolerance of the County Entity, and is considered along with other types of risks to ensure mission/business success.

    b. Each County Entity must designate an individual or group to be responsible for or assist in the technical information security function. For purposes of this policy, the Department of Information Services shall serve as the designee for the technical information security function for all county departments. Other entities (such as local governments/agencies, consultants, vendors, contractors, including their employees and subcontractors), that use or access any County IT resource for which the UCIS has administrative responsibility, must designate an individual or group to be responsible for the information security management function. This policy will refer to the individual or group designated as the Information Security Officer (ISO) or designated security representative. This function is responsible for evaluating and advising on information security risks. For County Entity's that are UCIS-supported agencies, the ISO function may be fulfilled by a Cyber Security Team provided by UCIS.

2. Information security risk decisions must be made through consultation with both function areas described in paragraph 1, above.

3. Although the technical information security function may be outsourced to third parties, each County Entity retains overall responsibility for the security of the information that it owns. The function of the CRC must be performed within the County Entity.

4.2 Functional Responsibilities

4.2.1 County Entity management is responsible for:

1. Evaluating and accepting risk on behalf of the County Entity;

2. Identifying the County Entity's information security responsibilities and goals and integrating them into relevant processes;

3. supporting the consistent implementation of information security policies and standards;

4. supporting security through clear direction and demonstrated commitment of appropriate resources;

5. promoting awareness of information security best practices through the regular dissemination of materials provided by the ISO;

6. implementing a process for determining information classification and categorization, based on industry recommended practices, County directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;

7. implementing the process for information asset identification, handling, use, transmission, and disposal, based on information classification and categorization;

8. determining who, within the County Entity, will be assigned and serve as information owners while maintaining ultimate responsibility for the Confidentiality, Integrity and Availability data;

9. participating in the response to security incidents;

10. complying with applicable notification requirements in the event of a breach of Personal, Private, Sensitive Information;

11. adhering to specific legal and regulatory requirements related to information security;

12. communicating legal and regulatory requirements to the ISO;

13. communicating the requirements of this policy and the associated

standards, including the consequences of non-compliance, to the County Entity workforce and third parties, and addressing adherence in third party agreements; and

14. establishment and testing of contingency plans as outlined in Section 4.15.18.

4.2.2 The ISO is responsible for:

1. Maintaining familiarity with County Entity business functions and requirements;
2. maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education credits directly related to information security;
3. assessing County Entity compliance with information security policies and, and in conjunction with the County Entity's Counsel, legal and regulatory information security requirements;
4. evaluating information security risks and assisting the County Entity in understanding information security risks and how to appropriately manage those risks;
5. representing and ensuring security architecture considerations are addressed;
6. advising on security issues related to procurement of products and services;
7. raising security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;
8. disseminating threat information to appropriate parties;
9. participating in the response to potential security incidents;
10. participating in the development of enterprise policies and standards for NYS that consider County Entity needs; and
11. promoting information security awareness.

4.2.3 IT management is responsible for:

1. Supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;
2. providing resources needed to maintain a level of information security control consistent with this policy;
3. identifying and implementing all processes, policies, and controls relative to security requirements defined by the County Entity's business and this policy;
4. implementing the proper controls for information owned by the County

Entity based on the County Entity's classification designations;

5. providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);

6. fostering the participation of information security staff and technical staff in protecting information assets, and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures; and

7. implementing business continuity and disaster recovery plans as referenced in Section 4.15. subsection 18.

4.2.4 The County Entity workforce is responsible for:

1. Understanding the baseline information security controls necessary to protect the Confidentiality, Integrity and Availability of information entrusted to County Entities;

2. protecting County information and resources from unauthorized use or disclosure;

3. protecting Personal, Private, Sensitive Information unauthorized use or disclosure;

4. abiding by UCIS Acceptable Use of Information Technology Resources and

5. reporting suspected information security incidents or weaknesses to the appropriate manager and ISO.

4.2.5 The UCIS Information Security Office (UCIS ISO) is responsible for:

1. Providing in-house expertise as information security consultants to the County Entities as needed;

2. developing the County's information security program and strategy, including measures of effectiveness;

3. establishing and maintaining the County's information security policy and standards;

4. assessing County Entity compliance with information security policies and standards;

5. advising on secure system engineering;

6. providing incident response coordination and expertise;

7. monitoring County networks for anomalies;

8. monitoring external sources for indications of County Entity data breaches, defacements, etc.

9. maintaining ongoing contact with security groups/associations and relevant

authorities;

10. providing timely notification of current threats and vulnerabilities; and

11. providing awareness materials and training resources.

4.3 Separation of Duties

1. To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.
2. Whenever separation of duties is not technically feasible, other compensatory controls must be documented and implemented, such as monitoring of activities, audit trails, and management supervision.
3. The audit and approval of information security controls must always remain independent and segregated from the implementation of said controls.

4.4 Information Risk Management

1. Any system or process that supports County Entity business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.

2. Risk assessments are required for new projects, implementation of new technologies, any significant updates, or changes to the operating environment, or in response to the discovery of significant vulnerabilities. Risk assessments are required regardless of whether the work is done by the County Entity, a vendor/contractor, or any other third party on behalf of the County Entity.

3. County Entites are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.

4. Risk assessments must include additional considerations when systems, services, or information will reside, or be accessed from, outside of the Contiguous United States to ensure compliance with relevant statutory, regulatory, and contractual requirements.

4.5 Information Classification and Handling

1. All information that is created, acquired, or used in support of County Entity business activities must only be used for its intended business purpose.

2. All information assets must have an information owner established within the County Entity’s lines of business.

3. Information must be properly managed from its creation, through authorized use, to proper disposal.

4. All information assets must be reviewed and reclassified (if needed) on a recurring basis, with a frequency determined by the County Entity. Any changes to the individual data elements of an information asset requires an immediate review.

5. An information asset must be classified according to the most sensitive type of data it contains

   a. If the County Entity is unable to determine the confidentiality classification of information, then it must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.

6. Merging of information that creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.

7. All reproductions of information must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.

8. Each classification has an approved set of baseline controls designed to protect the data asset and is aligned with NIST 800-53B Control Baselines for Information Systems and Organizations. These controls must be evaluated, tailored, and implemented to meet business requirements.

9. The County Entity must communicate the requirements for secure handling of information to its workforce.

10. A written or electronic inventory of all County Entity information assets must be maintained by the County Entity.

4.6 Information Sharing

1. CE content made available to the general public must be reviewed according to a process defined and approved by the County Entity. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.

2. Personal, Private, Sensitive Information must not be made available without appropriate safeguards approved by the County Entity.

3. For non-public information to be released outside a County Entity or shared among County Enties, a process must be established that, at a minimum:

   a. Ensures that an information classification has been performed and documented for the information to be released or shared;

   b. documents the intended use of the information;

   c. identifies the responsibilities of each party for protecting the information;

   d. defines the process and minimum controls required to transmit, store, and use the information;

e. records the measures that each party has in place to protect the information;

f. defines a method for compliance measurement;

g. provides a signoff procedure for each party to accept responsibilities;

h. establishes a schedule and procedure for reviewing the controls;

i. establishes procedures in response to a data breach, as detailed in subsection 4.9 below; and

j. identifies an end date for the use of the information (if applicable).

4. In addition to the requirements in Section 4.6.3, when information classified as having a High Confidentiality requirement is to be released or shared with outside parties, the CEs must ensure that they:

   a. Have in place, prior to sharing the information, a formal written agreement (e.g., Non-Disclosure Agreement, Acceptable Use Policy, Memorandum of Understanding, (etc.), which contains the requirements for the handling of information designate the level of management who can give written approval for:

      i. the transportation or storage of information outside of an approved storage facility;

      ii. the transmission of information outside the County Entity.

4.7 IT Asset Management

1. All IT hardware and software assets must be assigned by the County Entity to a designated business unit or individual within the County Entity.

2. County Entites are required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.

3. Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

4.8 Personnel Security

1. The County Entity workforce must receive, within 30 days of hire, general information security-awareness training that includes recognizing and reporting insider threats. Additional training on County Entity specific information security procedures, if required, must be completed before access is provided to specific County Entity's-sensitive information not covered in the general information security training. All information security

training must be reinforced at least annually and must be tracked by the County Entities.

2. A County Entities must require its workforce to abide by the UCIS Acceptable Use of Information Technology Resources, and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements.

3. All job positions must be evaluated by the County Entity to determine whether they require access to sensitive information and/or sensitive information technology assets.

4. For those job positions requiring access to sensitive information and sensitive information technology assets, County Entities must conduct workforce suitability determinations unless prohibited from doing so by law, regulation, or contract.

5. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state, and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for the County Entity to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the County.

6. A process must be established within the County Entity to repeat or review suitability determinations periodically and upon change of job duties or position.

7. County Entites are responsible for ensuring all County-issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

4.9 Information Security Incident Management

1. County Entities must have an incident response plan, consistent with New York State and Ulster County standards, to effectively respond to information security incidents.
2. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the ISO as quickly as possible. However, if a member of the workforce feels that information security concerns are not being appropriately addressed, they may confidentially contact the Cyber Incident Response Support for NYS Local Governments as describe below.

3. The Cyber Incident Response Support for NYS Local Governments must be notified as soon as possible of any information security incident that may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.

4.10 Physical and Environmental Security

1. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.
2. A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary.
3. Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities, such as electrical supply and cabling infrastructure.
4. All information technology equipment and information media must be secured and concealed to the extent possible to prevent a compromise of Confidentiality, Integrity, and Availability.
5. Visitors to information processing and storage facilities, including maintenance personnel, must be escorted at all times. Any maintenance performed remotely must be monitored by approved County staff.
6. For County Entity information that has a High Confidentiality requirement, written procedures must be created and implemented to keep track of individual documents, files, devices, or media, and the individuals who have possession of them.

4.11 Account Management and Access Control

1. All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the business unit and information technology (IT) unit.
2. Access to systems must be provided through the use of individually assigned, unique identifiers (user-IDs).
3. Associated with each user-ID is an authentication token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access.
4. Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock.
5. Tokens used to authenticate a person, or process must be treated as confidential and must be protected appropriately.

6. Tokens must not be stored on paper, or in an electronic file, hand-held device, or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the ISO.

7. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (e.g., read, update, etc.).

8. Access privileges will be granted by the County Entity in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with County Entity's missions and business functions (i.e., least privilege).

9. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).

10. Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for County Entity business or other approved use consistent with County Entity policy; that user activities may be monitored; and that the user should have no expectation of privacy. Users are required to acknowledge and agree to these logon banners prior to continued use of County Entity systems.

11. Advance approval for any remote-access connection must be provided by the County Entity. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved, and the contractual, process, and technical controls required for such connection to take place.

12. All remote connections must be made through managed points-of-entry reviewed by the ISO.

13. Remote work must be authorized, and data protection practices must be implemented to ensure appropriate protection of data prior to the individual being granted remote access. In addition, working remotely from international locations outside of the Contiguous United States may require special legal, human resource, and security considerations, and should only be allowed after careful County Entity analysis of these risks.

4.12 Systems Security

1. Systems include but are not limited to servers, platforms, networks, electronic communications, databases, and software applications.

   a. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of Ulster County. A list of assigned individuals or groups must be centrally maintained.

   b. Information security must be considered at system inception and documented as part of the decision to create or modify a system.

c. Each system must have a set of controls commensurate with the classification of any information that is stored on or passes through the system.

d. All system clocks must synchronize to a centralized reference time source set to Coordinated Universal Time, which is itself synchronized to at least three synchronized time sources.

e. Environments and test plans must be established to validate the system works as intended prior to deployment in production.

f. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels).

g. Formal change control procedures for all systems must be developed, implemented, and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.

h. For databases and software (including in-house or third party-developed and commercial off-the-shelf):

  i. All software written for, or to be deployed on, County Entity systems must incorporate secure coding practices prior to deployment to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats.

  ii. Once test data is developed, it must be protected and controlled for the life of the testing in accordance with the classification of the data.

  iii. Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:

  - All security controls applied to production data—including access restrictions, system configurations, and logging requirements—shall also be enforced in the test environment, and all test data shall be deleted immediately upon completion of testing; or
  - Sensitive data is masked or overwritten with fictional information.

  iv. Where technically feasible, development software and tools must not be maintained on production systems.

  v. Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.

  vi. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.

  vii. Privileged access to production systems by development staff must be restricted to those with a verifiable need.

viii. Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

2. <u>Network Systems:</u>

a. Connections between systems must be authorized by County Entity executive management and protected through implementation of appropriate controls.

b. All connections and their configurations must be documented. The documentation must be reviewed by the information owner and the ISO annually, at a minimum, to ensure:

i. The business case for the connection is still valid and the connection is still required;

ii. the security controls in place (e.g., filters, rules, access control lists, etc.) are appropriate and functioning correctly.

c. A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:

i. Internet accessible systems and internal systems;

ii. systems with high security categorizations (e.g., mission critical, systems containing Personal, Private, Sensitive Information) and other systems; and

iii. user and server segments.

d. Network management must be performed from a secure, dedicated network.

e. Authentication is required for all users connecting to County internal systems.

f. Network authentication is required for all devices connecting to County internal networks.

g. Only County Entity-authorized individuals or business units may capture or monitor network traffic.

h. A risk assessment must be performed in consultation with the County Entity ISO before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

4.13 Collaborative Computing Devices

1. Collaborative computing devices must:

a. Prohibit remote activation;

b. provide users physically present at the devices with an explicit indication of use.

2. County Entity's must provide simple methods to physically disconnect collaborative computing devices.

4.14 Vulnerability Management

1. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.

2. Systems may be subject to penetration testing based on the system's business criticality, legal or regulatory compliance requirements, data classification ratings, frequency, or other criteria as defined by the County Entity.

3. Where a County Entity has outsourced a system to another County Entity or a third party, vulnerability scanning and penetration testing must be coordinated.

4. Vulnerability scanning, penetration testing, and mitigation provisions must be included in third party agreements.

5. The output of the vulnerability scans and penetration tests must be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the ISO for the evaluation of risk.

6. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created and updated accordingly to document the planned remedial actions to mitigate vulnerabilities.

7. Any vulnerability scanning or penetration testing must be conducted by individuals who are authorized by the ISO. The ISO must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning or penetration testing will be deemed an unauthorized access attempt. The UCIS ISO must authorize vulnerability and penetration testing for utilization of UCIS-administered systems, infrastructure, or data centers. Anyone authorized to perform vulnerability scanning and penetration testing must have a formal process defined, tested, to be followed at all times to minimize the possibility of disruption.

4.15 Operations Security

1. All systems, and the physical facilities in which they are stored, must have documented operating instructions, management processes, and formal incident management procedures related to information security matters that define roles and responsibilities of affected individuals who operate or use them.

2. Any systems or services operated outside of the Contiguous United States

must not connect to internal County networks or the County data center.

a. Access to County systems or data outside the Contiguous U.S. by County employees and all third parties working on the behalf of a County Entity will by default be denied. Exceptions must be requested through the ISO office.

b. Accessing public data available on County websites or accessing citizen-facing County services is permitted from any location, unless otherwise determined by the County Entity.

3. System configurations must follow approved configuration standards.

4. Advanced planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.

5. Where a County Entity provides a server, application, or network service to another County Entity, operational and management responsibilities must be coordinated by all affected County Entities.

6. Host-based firewalls must be installed and enabled on all County Entity workstations to protect from threats and to restrict access to the minimum necessary. Controls must be implemented (e.g., anti-virus, end-point protection, software integrity checkers, web filtering, etc.,) across County Entity systems where technically feasible to prevent and detect the introduction of malicious code or other threats.

7. Controls must be implemented to stop content from running automatically from removable media (such as USB flash drives, external hard drives, CDs and DVDs, and memory cards).

8. Controls must be implemented to limit storage of County Entity information to County Entity authorized locations.

9. Controls must be in place to allow only County Entity-approved software to run on a system and to prevent execution of all other software.

10. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.

11. All security patches must be reviewed, evaluated, and appropriately applied in a timely manner. This process must be automated, where technically possible.

12. Any system, software, or Operating System environment that is no longer supported and cannot be patched to current versions (e.g. end-of-life hardware/software) must be decommissioned and removed from service.

13. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy and must record events to provide evidence and to reconstruct lost or damaged information.

14. Audit logs recording exceptions and other information security-relevant events must be produced, protected, and kept consistent with CE record retention schedules and requirements.

15. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound, and internal network traffic.

16. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.

17. Contingency plans must be established and tested regularly to help ensure a swift recovery of information systems after a disruption. There are several types of plans that cover specific operational areas. Types of contingency plans include but are not limited to the following:

    a. Business Continuity Plan: Provides procedures for sustaining mission/business operations while recovering from a significant disruption.

    b. Continuity of Operations Plan: Provides procedures and guidance to sustain an organization's mission essential functions (MEFs) at an alternate site.

    c. Disaster Recovery Plan: Provides procedures for restoring information systems operations.

    d. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).

    e. Recovery Time Objectives/Recovery Point Objectives for all critical systems.

18. Backup copies of County Entity information, software, and system images must be taken regularly in accordance with County Entity defined requirements.

19. Backups and restoration must be tested regularly. Separation of duties must be applied to these functions.

20. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

4.16 Citizens' Cybersecurity Notification

1. All County Entities are required under the HIPAA Breach Notification Rule, NYS SHIELD Act and NYS Department of State Data Breach Management to notify an individual when there has been, or is reasonably believed to have been, a compromise of the individual's private information.

2. This policy also applies to information maintained on behalf of a County Entity by a third party.

3. The County Entity must consult with the ISO to help determine the scope of the breach and restoration measures.

5.0 Compliance

This policy shall take effect upon publication. Compliance is required with all enterprise policies and standards. UCIS may amend its policies and standards at any time; compliance with amended policies and standards is required.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, County Entities shall request an exception through the ISO.

Any violation of this policy may subject the user to administrative action, civil penalties, and/or criminal prosecution. The CE will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in https://ulstercountyny.gov/ucis/IT-glossary-terms.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Information Security Office Reference:

Ulster County Information Services
25 South Manor Avenue
Kingston, NY 12401
Telephone: (845) 334-5300
Email: UCIS@co.ulster.ny.us

8.0 Revision History

This policy shall be reviewed at least once every 2 years to ensure relevancy.

Date	Description of Change	Reviewer
XX/YY/2025	Original Policy Release. UC Resolution number xxxxxxx adopted on MM/DD/YYYY	ISO

9.0 Related Documents

National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

International Standard ISO/IEC 27002, Information Security, Cybersecurity and Privacy Protection – Information Security Controls

SANS Institute, CIS Controls v8

NYS Technology Law, Article II, Internet Security and Privacy Act

Internal Revenue Service Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies

National Institute of Standards and Technology (NIST) SP 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems

National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) 2.0

Appendix A

Cyber Risk Coordinator Description

As outlined in Section 4.1., CEs must designate an individual or group to be responsible for cyber-related risk management. The Cyber Risk Coordinator (CRC) is the CE-assigned individual who ensures that cyber-related risk is managed within an CE. Organizations can implement this role either as a function of a current role (e.g., counsel, internal controls, etc.), or by creating a new role. The CRC must understand the CE's strategic goals and objectives. This individual should be either authorized to or made able to facilitate risk- based decision making, working with executive leadership. Where cybersecurity is a shared responsibility between CEs and UCIS, the CE is responsible for managing security requirements and risk, by performing and/or participating in the following functions:

- Identification of critical assets
- Data classification
- Account management and control of agency resources
- Incident response and management
- Employee awareness and training
- Developing requirements for systems that support business functions
- Preparation and review of agency policies and procedures
- Disaster Recovery & Business Continuity planning
- Routine assessments where the CE must play a lead role (e.g., annual Nationwide Cybersecurity Review)