County of Clinton
Information Technology Policy

Information Security Policy

Adopted: **June 9, 2021**

1.0 Purpose and Benefits

This policy defines the mandatory minimum information security requirements for the County of Clinton (County) and its component departments and agencies (departments), as defined below in Section 3.0 Scope. Any department may, based on its individual business needs and specific legal, state, and federal requirements, exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this policy.

This policy acts as an umbrella document to all other security policies and associated standards. This policy defines the responsibility to:

- protect and maintain the confidentiality, integrity, and availability of information and related information technology assets;
- manage the risk of security exposure or compromise;
- assure 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.

This policy benefits the County and its departments by defining a framework which will assure appropriate measures are in place to protect the confidentiality, integrity and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect information.

2.0 Authority

This policy has been created by the Clinton County Department of Information Technology, under the direction of the Director of Information Technology, and approved under the authority of the Clinton County Legislature.

3.0 Scope

This policy encompasses all systems, automated and manual, for which the County or department has administrative responsibility, including systems managed or hosted by third parties on behalf of the County. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

4.0 Information Statement

4.1 Organizational Security

a. The Clinton County Director of Information Technology (IT Director), or their designee, shall function as the Clinton County Chief Information Security Officer (CISO).
b. The Clinton County Director of Information Technology shall designate an individual to function as the Clinton County Information Security Officer (ISO).
c. Information security requires both an information risk management function and an information technology security function.
    1. Each department must designate an individual or group to be responsible for the information risk management function, assuring that:
        i. risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed as an enterprise with regard to the overall strategic goals and objectives of carrying out the department's core missions and business functions; and
        ii. the management of information assets and information system-related security risks is consistent, reflects the risk tolerance, and is considered along with other types of risks, to ensure mission/business success.
    2. The ISO shall be responsible for the technical information security function. The Director of IT may designate additional individuals to assist the ISO with this function. For purposes of clarity and readability, this policy will refer to the ISO and individuals designated as the Information Security Officer (ISO)/designated security representatives. This function will be responsible for evaluating and advising on information security risks, and implementing required information security controls.
d. Information security risk decisions must be made through consultation with both function areas described in c. above.
e. Although the technical information security function is led by the ISO, and may include third parties, each department retains overall responsibility for the security of the information that it owns.

4.2 Functional Responsibilities

4.2.1 Department Management is responsible for:

1. evaluating and accepting risk on behalf of the department;
2. identifying departmental 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 CISO, ISO/designated security representatives, and IT Director;
6. implementing the process for determining information classification and categorization based on industry recommended practices, organization policies and 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 will be assigned to serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;
9. participating in the response to security incidents;
10. complying with notification requirements in the event of a breach of private information;
11. adhering to specific legal and regulatory requirements related to information security;
12. communicating the department's objectives and activities, its place in critical infrastructure, and its role in the supply chain to the IT Director, CISO, and ISO/designated security representatives;
13. communicating legal and regulatory requirements to the ISO/designated security representatives;
14. communicating the requirements of this policy and its associated policies and standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements; and
15. responding completely and accurately to any public records request for any information asset which constitutes a public record.

4.2.2 The ISO/designated security representatives are responsible for:

1. maintaining familiarity with business functions and requirements;
2. maintaining an adequate level of current knowledge and proficiency in information security;
3. assessing compliance with information security policies and legal and regulatory information security requirements;
4. evaluating and understanding information security risks and how to appropriately manage those risks;
5. representing and assuring security architecture considerations are addressed;
6. advising on security issues related to procurement of products and services;
7. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;
8. registering for, and receiving, cyber threat intelligence from known, trusted sources;
9. disseminating threat information to appropriate parties;
10. participating in the response to potential security incidents;
11. participating in the development of enterprise policies and standards that considers the County's and departments' needs; and
12. promoting information security awareness.

4.2.3 The Director of Information Technology 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 business and this policy;
4. implementing the proper controls for information owned based on the classification designations;
5. providing training to appropriate technical staff on secure operations (e.g., secure coding and configuration);
6. fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures;
7. establishing incident response plans and business continuity/disaster recovery plans for systems managed by the County Department of Information Technology;, and
8. establishing all information security standards and procedures required to comply with County information security policies, including, but not limited to:
    a. Account Management and Access Control Standard
    b. Password and Authentication Standard
    c. Physical Environment for Information Technology Standard
    d. Secure Data Transmission Standard
    e. Secure Logging Standard

4.2.4 The workforce is responsible for:

1. understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted;
2. protecting information and resources from unauthorized use or disclosure;
3. protecting personal, private, sensitive information from unauthorized use or disclosure;
4. abiding by the Acceptable Use of Information Technology Resources Policy (AUP);
5. reporting suspected information security incidents or weaknesses to the appropriate manager and ISO/designated security representatives.

4.2.5 Third-parties providing services to, or on behalf of, the County are responsible for:

1. evaluating and reporting the risk associated with their services to County or department management;
2. protecting County information associated with, or processed by, their services from unauthorized use or disclosure;
3. cooperating with County information security personnel with required audits, vulnerability testing, and response and recovery testing and planning;
4. monitoring their services for vulnerabilities, compromise, and other cybersecurity events;

5. promptly reporting suspected information security incidents or weaknesses to the appropriate County or department manager, and the ISO/designated security representatives.

4.2.6 The CISO is responsible for:

1. providing in-house expertise as security consultant as needed;
2. developing the security program and strategy, including measures of effectiveness;
3. maintaining County information security policies;
4. reviewing information security standards, procedures, and plans to verify compliance with County information security policies;
5. assessing compliance with security policies and standards;
6. advising on secure system engineering;
7. providing incident response coordination and expertise;
8. monitoring networks for anomalies;
9. monitoring external sources for indications of data breaches, defacements, etc.
10. maintaining ongoing contact with security groups/associations and relevant authorities;
11. providing timely notification of current threats and vulnerabilities; and
12. providing awareness materials and training resources.

4.2.7 The Clinton County Legislature is responsible for:

1. reviewing and providing approval for proposed County information security policies.

4.3 Information Risk Management

a. Any system or process that supports business functions must be appropriately managed for information risk and undergo information security risk assessments, at a minimum annually.
b. Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.
c. Departments are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.
d. Risk assessment results, and the decisions made based on these results, must be documented and submitted to the ISO for review.

4.4 Information Classification and Handling

a. All information, which is created, acquired, or used in support of business activities, must only be used for its intended business purpose.
b. All information assets must have an information owner established within the lines of business.
c. All Information must be properly managed from its creation, through authorized use, to proper disposal.
d. All information must be classified on an ongoing basis based on its confidentiality, integrity and availability characteristics.
e. An information asset must be classified based on the highest level necessitated by its individual data elements.

f. If the department is unable to determine the confidentiality classification of information, or the information contains personal identifying information (PII), the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.
g. 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.
h. All reproductions of information in their entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.
i. Each classification must have an approved set of baseline controls designed to protect these classifications and these controls must be followed.
j. Departments must communicate the requirements for secure handling of information to their workforce.
k. A written or electronic inventory of all information assets must be maintained.
l. Content made available to the general public must be reviewed according to a process that will be defined and approved by the County. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.
m. PII must not be made available without appropriate safeguards approved by both the Department Head and Director of IT.
n. For non-public information to be released outside the County or shared between departments, a process must be established that, at a minimum:
    1. evaluates and documents the sensitivity of the information to be released or shared;
    2. identifies the responsibilities of each party for protecting the information; and,
    3. complies with County IT standards for the transmission of non-public information.
o. All information assets must be maintained in accordance with their respective records retention schedules and all applicable Federal, State, and Local regulations.

4.5 IT Asset Management

a. All IT hardware and software assets must be assigned to a department, departmental business unit, or individual.
b. A master inventory of all internal and external County hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of detail deemed necessary for tracking and reporting, must be kept by County IT. This inventory must be automated where technically feasible. When County IT does not have administrative responsibility for a department asset, departments must provide County IT all information required to maintain the asset inventory.
c. Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.
d. All hardware assets which access County or department information assets must be centrally managed using a method approved by the IT Director.
e. Maintenance, including the repair, of information assets must only be performed by authorized personnel using approved tools. All maintenance must be logged in accordance with the Secure

Logging Standard. Remote maintenance of assets is permitted in accordance with the Remote Access Policy.

4.6 Personnel Security

a. All employees must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to sensitive information not covered in the general security training.
b. The County must require its workforce to abide by the Acceptable Use of Information Technology Resources Policy and an auditable process must be in place for users to acknowledge they agree to abide by the policy's requirements.
c. All job positions must be evaluated by the Department Head, or their designee, to determine whether they require access to sensitive information and/or sensitive information technology assets.
d. For those job positions requiring access to sensitive information and sensitive information technology assets, departments must conduct workforce suitability determinations, unless prohibited from doing so by law, regulation, or contract.
e. A process must be established within the department to repeat or review suitability determinations periodically and upon change of job duties or position.
f. Departments are responsible for ensuring all issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

4.7 Cyber Incident Management

a. The County must have an incident response plan, consistent with County policies and standards, to effectively respond to security incidents. The incident response plan must be tested regularly.
b. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the ISO/designated security representatives as quickly as possible. If a member of the workforce feels cyber security concerns are not being appropriately addressed, they may confidentially contact the CISO directly.
c. The CISO must be notified of any cyber incident which 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.

4.8 Physical and Environmental Security

a. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.
b. 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. These measures must be implemented to mitigate the risks.
c. 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.

d. All information technology equipment and information media must be secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of information contained therein.
e. Access to information processing and storage facilities must be tracked in accordance with the Physical Environment for Information Technology Standard.

4.9 Account Management and Access Control

a. All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the department and County IT.
b. Except as described in the, Account Management/Access Control Standard, access to systems must be provided through the use of individually assigned unique identifiers, known as user-IDs.
c. 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.
d. Methods and levels of authentication must comply with the Password and Authentication Standard.
e. 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.
f. Automated techniques and controls must be implemented to terminate a session after specific conditions are met as defined in the Account Management/Access Control Standard.
g. Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.
h. 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) is listed as an approved method in the Password and Authentication Standard.
i. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.).
j. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with department missions and business functions (i.e., least privilege).
k. Users of privileged accounts must be informed of, and understand, their roles and responsibilities regarding the use of their account. A separate, non-privileged account must be used to perform normal business transactions (e.g., accessing the Internet, e-mail).
l. Logon banners must be implemented on all systems where that feature exists to inform all users the system is for business or other approved use consistent with policy, user activities may be monitored, and the user should have no expectation of privacy.
m. Advance approval for any remote access connection must be provided by both the department head and IT Director. 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.
n. All remote connections must be made through managed points-of-entry reviewed by the ISO or CISO, and approved by the Director of IT.

o. Working from a remote location must be authorized by management and practices which assure the appropriate protection of data in remote environments must be shared with the individual prior to the individual being granted remote access.

4.10 Systems Security

a. Systems include but are not limited to servers, platforms, networks, communications, databases and software applications.
    1. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of the County or department. A list of assigned individuals or groups shall be centrally maintained by County IT.
    2. Security must be considered at system inception and documented as part of the decision to create or modify a system.
    3. Each system must have a set of controls commensurate with the classification of any data that is stored on or passes through the system.
    4. Resiliency requirements must be defined prior to system design and implementation.
    5. Where feasible, disparate services must be segmented onto separate systems. (i.e. principal of least functionality).
    6. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.
    7. 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.
        a. Databases and Software (including in-house or third party developed and commercial off the shelf (COTS):
            1. All software written for or deployed on systems must incorporate secure coding practices to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.
            2. Development and testing environment(s) must be separate from the production environment.
            3. 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.
            4. 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:
                i. All security measures, including but not limited to access controls, system configurations, and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or
                ii. sensitive data is masked or overwritten with fictional information.
            5. Where technically feasible, development software and tools must not be maintained on production systems.
            6. 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.

7. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
8. Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

b. Network Systems:
   1. Connections between systems must be authorized by the department management of all relevant departments and protected by the implementation of appropriate controls.
   2. All connections and their configurations must be documented and the documentation must be reviewed by the information owner and the ISO/designated security representatives annually, at a minimum, to assure:
      i. the business case for the connection is still valid and the connection is still required; and
      ii. the security controls in place (filters, rules, access control lists, etc.) are appropriate and functioning correctly.
   3. A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:
      i. Internet accessible systems and internal systems;
      ii. user and server segments;
      iii. control networks.
   4. Network management must be performed from a secure, dedicated network.
   5. Authentication is required for all users connecting to internal systems.
   6. Network authentication is required for all wireless devices connecting to internal networks.
   7. Only authorized individuals or business units may capture or monitor network traffic.
   8. A risk assessment must be performed in consultation with the ISO/designated security representatives before the initiation of, or significant change to, any network technology or project.

4.11 Collaborative Computing Devices

a. Collaborative computing devices, including devices such as networked white boards, smart displays, cameras, and microphones, must:
   1. prohibit remote activation; and
   2. provide users physically present at the devices with an explicit indication of use.

b. Simple methods to physically disconnect collaborative computing devices must be provided.

4.12 Vulnerability Management

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

c. All systems are subject to periodic penetration testing.

d. Penetration tests are required periodically for all critical environments/systems.

e. Where the department has outsourced a system to another department or a third party, vulnerability scanning/penetration testing must be coordinated.

f. Scanning/testing and mitigation must be included in third party agreements.
g. The output of the scans/penetration tests will be reviewed in a timely manner by the system administrator. Copies of the scan report/penetration test must be shared with the ISO/designated security representatives for evaluation of risk.
h. 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.
i. Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the ISO/designated security representatives. The CISO must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.
j. Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested, and followed at all times to minimize the possibility of disruption.
k. A process to document and track all vulnerabilities identified must be created.

4.13 Operations Security

a. 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 which define roles and responsibilities of affected individuals who operate or use them.
b. System configurations must follow approved configuration standards.
c. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis. Resources must be allocated based on system criticality.
d. Where the department provides a server, application or network service to another department, operational and management responsibilities must be coordinated by all impacted entities.
e. Host based firewalls must be installed and enabled on all workstations to protect from threats and to restrict access to only that which is needed.
f. Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across systems where technically feasible to prevent and detect the introduction of malicious code or other threats.
g. Controls must be implemented to disable automatic execution of content from removable media.
h. Controls must be implemented to limit storage of information to only authorized locations.
i. Controls must be in place to allow only approved software to run on a system and prevent execution of all other software.
j. All systems must be maintained at a vendor-supported level (i.e. firmware and software version level) to ensure accuracy and integrity.
k. All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically and financially feasible.
l. Systems which can no longer be supported or patched to current versions must be removed.

m. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy, and record events to provide evidence and to reconstruct lost or damaged data.
n. Audit logs recording exceptions and other security-relevant events must be produced, protected and kept consistent with record retention schedules and requirements.
o. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound and internal network traffic.
p. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.
q. Protection systems, including monitoring and detection systems, must be periodically reviewed for effectiveness, and improved where feasible. The efficacy of protection systems must be shared with appropriate stakeholders.
r. Contingency plans (e.g., business continuity plans, disaster recovery plans, and continuity of operations plans) must be established and tested regularly. At a minimum, these plans must include:
    1. The dependencies and critical functions required for the delivery of critical services.
    2. 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).
    3. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.
s. Backup copies of department information, software, and system images must be taken regularly in accordance with the department's defined requirements. Whenever possible, backups should be centralized with County IT. Departments shall provide County IT with installation packages and/or system images when systems are installed by department staff or third-parties.
t. Backups and restoration must be tested regularly.
u. 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.

5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all County policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, departments shall request an exception through the Chief Information Security Officer's exception process.

6.0 Definitions of Key Terms

Term	Definition

Authentication Token	An information asset, either physical or virtual, used to verify a user's identity. Examples include passwords, biometric data (fingerprint, retina scan), and hardware security keys.
Collaborative Computing Device	Collaborative computing devices may include, but are not limited to, networked white boards, cameras, and microphones that are connected to County systems for the purposes of conducting government business collaboratively.
Critical Infrastructure	The systems which, when destroyed or incapacitated, would have a severe impact on the security, financial security, health, or safely of the County or County residents.
Information Asset	A defined collection of data, stored in any manner and managed as a single unit, used for the purpose of enabling the County or department to perform its business functions.
Penetration Test	A test of the overall strength of a system's defenses by simulating the objectives and actions of an attacker.
Personal Identifying Information (PII)	Information that can be used to distinguish a person's identity as defined by New York State Technology Law. This includes an individual's: • social security number; • driver's license number or non-driver identification card number; • account number, credit, or debit card number in combination with other identifiable data; • biometric information such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation; and, • user name or email address in combination with a password or security question.
Recovery Point Objective	The maximum amount of data, as a measurement of time, which can be lost after an event before significant harm is caused to business operations.
Recovery Time Objective	The maximum amount of time for which a system can be down before significant hard is caused to business operations.
Remote Access	Access to any system for which the County or department has administrative responsibility, including systems managed or hosted by third parties on behalf of the County, from outside the County's trusted Local Area Network (LAN).

7.0 Contact Information

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

Director of Information Technology
Clinton County Department of Information Technology
137 Margaret Street, Suite 202
Plattsburgh, NY 12901

8.0 Revision History

This policy shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
06/09/2021	**Initial policy adoption**	**David Randall, Director of Information Technology**

9.0 Related Documents

- Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (National Institute of Standards and Technology)
- Retention and Disposition Schedule for New York Local Government Records (LGS-1)
- New York State Technology Law, Article II, Internet Security and Privacy Act