Oneida County Information Security Policy

Approved by the Oneida County Board of Legislators

June 8, 2022

Oneida County Information Security Policy

1 Contents

2 Purpose

Access to Oneida County's (hereinafter referred to as the County) Information System has been provided to authorized County Users for the purpose of providing service to the County. All Users have a responsibility to maintain and protect the County's Information Assets against accidental or intentional disclosure or compromise. Each user also has the responsibility to maintain and protect the County's public image and to use the County's Information System in a legal/ethical manner consistent with County and department policies.

Information is essential to all services the County provides. As a result, Information Security is a critical factor in the delivery of County services. The integrity, availability, and confidentiality of County information collected, processed, and stored needs to be ensured. The accidental or intentional disclosure of non-public County information can have serious repercussions. The County, in the event its Information resources are compromised due to user misconduct, can face legal liability associated with the disclosure of information governed by federal and state laws (e.g., Health Insurance Portability Accountability Act of 1996 (HIPAA)).

To ensure that the County's Information resources are used in a responsible and productive manner, the following policy for using the County's Information Systems has been established.

- **Effective Date**: the Oneida County Board of Legislators, effective June 8, 2022 originally approved this policy.
- **Policy Review**: This policy will be reviewed at least annually at the discretion of the Chief Information Security Officer (CISO), in conjunction with any necessary resources including, but not limited to, Oneida County's Current Information Security vendor. It will also be reviewed immediately after the appropriate response has been completed for a confirmed Cyber Security Incident.
- **Expiration Date**: This policy shall remain in effect until superseded, amended, or cancelled.

All use of Information Systems involves certain risks that must be addressed through proper controls. The protective requirements for each of the individual Information Systems within the County will vary according to the unique characteristics of the system, data sensitivity and mission- related criticality of the System or Information. Appropriate levels of security and cost-effective controls, which are adequate to achieve an acceptable level of risk for each system, will be implemented through the guidance of this policy.

The policy ensures that all Users are knowledgeable of acceptable behavior when using the County's Information Systems, understand their Information Security responsibilities and are held accountable.

Furthermore, the policy ensures that the County will protect and maintain the availability, integrity, confidentiality and non-repudiation of Information and Information resources. Effective information security is a team effort involving all Users who come in contact with Information and Information resources. In recognition of the need for teamwork, this policy clarifies responsibilities and duties associated with Information Security.

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 operation. Require that all Users who use the County's Information Systems:
    a. Will be knowledgeable of acceptable County Information System usage,
    b. Will understand their Information Security responsibilities, and
    c. Will be 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 may 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.

3 Scope

The policies contained in this document are applicable to all of the County's internal computer networks (County Wide Area Network [WAN]), interconnections with systems outside the County WAN (e.g., the Internet), and all other County Information System resources, whether located within the physical confines of County property or at an off-site location. They cover all computer and communication devices (e.g., routers, modems, TDDs, radios, phones) owned or operated by the County. They also cover any computer or communications device that is present on County premises and/or connected to County Information Systems, but which may not be owned or operated by the County.

These policies are mandatory for all County organizational units, County staff, and other authorized Users having access to and/or using the Information Systems and resources of the County.

4 Organization of the Information Security Policy

The County's Information Security Policy is comprised of two parts: Managerial Policy and Technical Policy. The Managerial Policy discusses policy related to use, ownership, management, disclosure and processing information on the County's Information Systems. Technical Policy discusses the policy related to the technical aspects of the County's Information Security.

5 PART I: Managerial Policy

5.1 Information Technology Asset Inventory

An inventory of Information Systems detailing all hardware, software, communication links, sensitive data and names of Users will be maintained by IT on an ongoing basis and reviewed at least annually at the direction of the CISO. Inventory format will be determined by County IT management.

5.2 County Information Security Administration

5.2.1 Centralized Responsibility for Information Security

The responsibility and authority for the County's Information Security is formalized in the Chief Information Security Official (CISO). The CISO is responsible for maintaining, coordinating, and directing specific actions that maintain the confidentiality, the integrity, the availability andthe non-repudiation of County Information resources as specified in this Policy. The CISO reports to the Oneida County Executive.

5.2.2 Information Services Network and Technical Support Team Responsibilities

Information Technology is responsible for maintaining the County's Information resources in a manner that is responsive to the County's business needs. These responsibilities include, but are not limited to:

1. Administer network, intranet, and internet operations in a secure manner;
2. Develop, implement and maintain a Strategic Information Systems Protection Plan (Information Security vision) for the County, to include secure network architecture, effective access control, virus/malicious code protection, process for implementing patches for vulnerabilities, Intrusion Detection, traffic screening and other Information Security measures;

3. Periodically audit the operations of all technical security measures in place to ensure the measures are operating as perceived;
4. Harden systems (by removing unnecessary services and patching necessary ones) before connecting them to the Internet;
5. Establish an integrated disaster recovery plan (contingency plan) to include regular backups of critical County data with offsite storage and regular testing of data restoration operations in accordance with department specific needs and resources;
6. Compile, maintain and protect documentation describing configuration and specific secure operating procedures for the County's Information Systems, as well as the County's internet operations;
7. Establish and maintain effective and secure telecommunications capabilities for/with off-site facilities;
8. Identify common User deficiencies and ensuring these are addressed in Information Security training;
9. Implement a secure system of identification and authentication to control access to County Information;
10. Complete a periodic review of assigned computer accounts to ensure access privileges are commensurate with User needs;
11. Implement judicious access control measures;
12. Install patches expeditiously to identified system exploits (vulnerabilities);
13. Educate Users on security issues;
14. Activate the security capabilities of the server and client systems over which they have authority;
15. Review logs in a timely manner – logs are to be reviewed upon updates/reboots/on error;
16. Other routine activities related to security.

5.2.3 Information Security Incident Response

5.2.3.1 Information Technology Cybersecurity Team

The County's Information Technology Cybersecurity Team (Cybersecurity Team) reporting to the CISO is charged with responding in a quick, effective, and orderly manner to all Information Security incidents on the County's Information infrastructure. The Cybersecurity Team is composed of staff from County IT and other individuals as designated by the CISO. The Cybersecurity Team is responsible for defining procedures for detecting, mitigating, investigating, implementing procedures and preventing such future incidents.

5.2.3.2 Secure Operations Center (SOC)

Oneida County utilizes Secure Operations Center (SOC) monitoring to ensure all potential cybersecurity Incidents or attacks are discovered and addressed effectively and efficiently. The SOC leverages monitoring tools and the County's third-party cybersecurity vendor to ensure operative monitoring is effective. The SOC monitoring team, at the discretion of the CISO, is responsible for alerting appropriate parties when an Incident takes place and beginning the Incident Response process in accordance with the Oneida County Incident Response Plan. Oneida County Information Technology retains a third-party cybersecurity vendor on an on-call basis for off-hours detection and response.

5.2.3.3 Incident Response Plan

All Security Incidents will be investigated, according to the Incident Response Plan and associated Incident Response procedures, to determine immediate actions needed as well as measures to secure the County's Information resources from further compromise. After a security Incident, the Cybersecurity Team will implement the following list of recovery actions to bring the affected system(s) on-line and into service:

1. Investigate how the Incident occurred;
2. Avoid escalation and further Incidents;
3. Assess the impact and damage of the Incident;
4. Recover from the Incident;
5. Identify the cause or source of Incident (if appropriate and possible);
6. Take actions to prevent and/or deter the action from recurring;
7. Document the Incident and preserve evidence where possible, for reporting purposes and effective resolution of an Incident.

The CISO, in conjunction with the County's cybersecurity vendor is responsible for the forensic analysis that needs to be done to clean the system in the event of a security Incident. The investigation will be documented so that evidence is not destroyed or modified in the course of the investigation that may hinder prosecution.

The investigation must provide sufficient information, so that IT can take steps to ensure that:

1. a similar Incident cannot reasonably take place on the County's information systems; and
2. security measures have been reestablished and strengthened

The findings of the Incident investigation will be documented in detail for future reference.

5.2.4 Annual Information Systems Planning Process Required

The CISO, in conjunction with the County's Cybersecurity Team shall annually review Information Security controls, addressing both the adequacy of controls and compliance with them, and prepare plans for the improvement of Information Security on the County's Information Systems in the wake of technological advances and the County's plan to incorporate new technology into the County's business processes. The developed plan will then be reviewed with the appropriate groups and committees.

5.2.5 Risk Analysis, Assessment and Management

The CISO shall perform a Risk Assessment on all applications, systems, and services to be deployed on the County's Information Systems. The analysis should include:

1. identification of threats and vulnerabilities;
2. identification of application owners;
3. analysis of the value of the Information;
4. identification of the impact on the County's operations in the event of a security compromise; classify the damage level: high, medium, low;
5. predict re-occurring possibility; and
6. an estimate of the cost of implementing security controls.

Based on the Risk Analysis, CISO in conjunction with the County's Cybersecurity Team, will implement security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level in compliance with HIPAA regulation §164.306(a), and other applicable state, federal and local laws and regulations.

5.2.6 Accrediting Hardware and Software

Information Technology is responsible for the accreditation of any new system, network, software or application before it is connected or placed onto the County's Information Systems. Accreditation is the process by which software and hardware are evaluated on whether they are consistent with the County's Information Security posture. This may require support from a 3rd party as it could require advanced technical knowledge of new or existing systems.

5.2.7 Configuration Control/Change Management

Information Technology will employ a documented change control process to ensure that only authorized changes are made on County Information Systems. This change management procedure will be used for all changes to software including planned and emergency changes including but not limited to upgrades and patches, hardware, communications links, etc.

5.2.8 Current Information Security Manual Required

The CISO must prepare, maintain, and distribute Information Security manual(s) describing the County's current Information Security Policies and procedures.

5.2.9 Amending the Information Security Policy

The County Information Security Policy shall be amended when there is a need to align policy to stay current with laws and regulations, technology, and County business practices. The CISO in conjunction with the County's Cybersecurity Team is responsible for drafting new policy statements or amendments to policy for review and approval by the Board of Legislators and County Executive. Once approved, the amended policy will be in effect.

5.3 User Responsibilities

All Users are responsible for maintaining the confidentiality, integrity and availability of the County's Information to facilitate effective and efficient conduct of County business.

Four responsibility Classifications **(compliance, department, custodian,** and **user)** are defined to assist Users in understanding their roles and responsibilities when using the County's Information Systems.

Compliance: Oneida County is required to comply with all federal, state and local laws pertaining to the protection of and use of Information residing on the County network. A Chief Compliance Officer appointed by the County Executive will be responsible for identifying all applicable mandates and legislation pertaining to Information resident on the County network or devices, overseeing and managing regulatory compliance and for providing direction and advice to County Officials and Departments Heads.

Department: All Information residing on the County's Information Systems belongs to a designated department. The Department Head (Elected Official, Commissioner or Director) shall be considered the owner of the Information and is responsible for decisions regarding Information residing within the department. The Department Head determines the appropriate Information Sensitivity Classification to be applied to the Information and is responsible for deciding which Users will be permitted to access the Information and how the Information will be used. The Department Head is responsible for ensuring employees are complying with all applicable regulations, internal policies

and procedures.

Custodian: Information on the County's Information Systems must have a designated custodian. The Custodian in the County is usually Information Technology (IT); however, other Custodians including vendors or contractors also exist. The Custodian is responsible for protecting the Information in accordance with the departments' access control, data sensitivity and data criticality instructions.

At a minimum, the Custodian is responsible for:

1. providing physical security for equipment, Information storage, backup, and recovery;
2. providing a secure processing environment that can adequately protect the integrity, confidentiality, and availability of Information;
3. developing a business continuity plan and contingency plan;
4. administering access to Information as authorized by the Information owner; and
5. implementing procedural safeguards and cost-effective controls.

User: The User, in addition to the definition stated in the Glossary of this Policy, is an individual or a group that has been authorized access to the Information asset by the Department Head. The User has the responsibility of using the Information only for the intended purpose – consistent with the Information owner's instructions – and safeguarding the integrity, confidentiality and availability of the Information accessed. Users are also responsible for familiarizing themselves andcomplying with the County's Information Security Policies.

Users are responsible for strictly adhering to the requirements set forth in the Oneida County Acceptable Use Policy as well as all security policies, procedures and controls governing the security of the Information resources under their control to prevent unauthorized disclosure of Information.

Each User is responsible for the content of all text, audio and images that they place or send over email, voicemail, and fax, the Intranet or Internet. No abusive, profane or offensive language shall be transmitted through County systems. Users who wish to express personal opinions on the Internet are not to do so using County resources or systems.

Information stored, processed and transmitted on the County's Information Systems are owned by the County, and, therefore, is a County resource in the custody of the User. It is the user's responsibility to ensure that all Sensitive County Information is adequately protected at all times – in the manner as prescribed by the User's department and County policy. When data is transferred from the User's custodial responsibility to another User, each User accepts the same responsibility for continued protection.

Users shall:

1. Protect others' Private Information and Confidentiality;
2. Consider organizational access before sending, filing, or destroying e-mail messages;
3. Remove messages, transient records, and reference copies in a timely manner;
4. Comply with department and unit/division policies, procedures, and standards;

5. Become cognizant of the Sensitivity/criticality of the Information they handle and apply appropriate protective measures when handling the Information;

6. Save ALL Data to a County network drive;

7. Save their work and log out of their network account at the end of each business day;
   a) Desktop Users are required to leave the PC powered on (log out but leave the power on!)

   b) Laptop Users are required to:

      i. shut down their laptop at the end of each business day;

      ii. take the home at the end of each business day, and

      iii. ensure that the laptop is connected to the network at least once each week to ensure important security patches are applied in a timely manner

8. Coordinate the connection of County-owned mobile devices (i.e. Smart Phones,Tablets, etc.) with IT;

9. Coordinate the connection of devices with RF (radio frequency) capabilities (e.g.,wireless access points, wireless LANs) with IT;

10. Not connect a modem to a phone line while the same computer is connected to the County LAN;

11. Not connect to the county network while being simultaneously connected to a MiFi device.

12. Use only software licensed to the County on County computers;

13. Use robust network passwords in accordance with the County Password Policy and change them immediately when required;

14. Never share ID or passwords with anyone else, including superiors and IT staff;

15. Never document passwords and put them on or near the computer (e.g., "sticky notes" under keyboards, on monitors, etc.);

16. Log off or activate screensavers with password protection to protect the County's Information when computers are left unattended for more than 10 minutes;

17. Never release non-public County Information without specific direction from the Department Head;

18. Not disclose Sensitive County data to other County staff other than on a need-to-know basis;

19. Secure any physical copies of sensitive County Data on media (i.e., USB or thumbdrives, dvd, etc.) and printouts when left unattended;

20. Immediately report indicators of virus infection and/or operational anomalies to IT;

21. Immediately report all discovered security vulnerabilities and/or computer security concerns to their supervisor and IT;

22. When working away from the office, take all appropriate measures consistentwith workplace procedures to safeguard access to County information resources (e.g., computers, networks, Data);

23. Never use County devices, systems/applications or network access for (Please see Oneida County Acceptable Use Policy Acceptable Use Policy):
    a) Activities unrelated to the County's mission/business;
    b) Activities unrelated to official assignments and/or job responsibilities;
    c) Any illegal purpose;
    d) The transmission of threatening, fraudulent, obscene or harassing materials or correspondence;
    e) Unauthorized distribution of County or New York State data and information;
    f) Interfering with or disrupting network Users, services or equipment;
    g) Private purposes such as marketing or business transactions;
    h) Solicitation for religious or political causes;
    i) Not-for-profit business activities inconsistent with the County's mission or unrelated to County business;
    j) Private advertising of products or services;
    k) For any activity meant to foster personal gain.
24. When sending confidential information, all files must be encrypted and a password sent via an alternate form of communication (text, IM, call, etc.). This applies even when sending a file through a secure network (e.g., HIN, HSEN, etc.). The County uses for secure email transmission.

5.4 Information Security Training and Awareness

5.4.1 Information Security Training

Users as employees, temporary worker and interns shall be provided with sufficient Information Security training and support reference materials appropriate to their role by their Department Head to meet their job responsibilities. IT will only establish User accounts and set up access to Sensitive Information at the specific direction of the Department Head who is responsible for ensuring User compliance with all federal, state, county and department policies governing the use, handling and protection of sensitive data. Users as contractors and/ or vendors shall be advised by the CISO of this Policy and shall ensure compliance with same.

5.4.2 Required Security Training

All Users shall be provided with sufficient Information Security training and support reference

materials to meet their job responsibilities. The Information Security training must be given before the User is allowed access to and use of the County's Information Systems. At the conclusion of the training, each User will be required to sign the Oneida County Acceptable Use Policy. If users do not complete required training, the CISO reserves the right to lock user access to the Oneida County network until all required training is completed.

5.4.3 Responsibility for Cyber Security Training

The CISO in conjunction with the County's cybersecurity vendor is responsible for developing cyber security awareness training materials and for ensuring training sessions for new Users and periodic refresher security training to remind all Users of their responsibility and obligations with respect to Information Security.

5.4.4 Information Security Awareness

The CISO in conjunction with the County's cybersecurity vendor is responsible for developing and conducting an Information Security awareness program throughout the year, annually.

5.5 Contingency Planning

5.5.1 Contingency and Disaster Planning Document

The County, as part of its preparedness against natural and man-made disasters, shall have a current documented and tested Continuity of Operations (COOP) and Disaster Recovery (DR) Plan for each department, which addresses the possibility of short and long-term loss of computing and networking services. The plan needs to take into consideration the criticality of the various systems. Such a plan needs to include all procedures and information necessary to return computing and networking systems to full operation in the event of a disaster. The plan must be communicated to, and approved by all those (especially the Department Head) who would be affected by such a disaster.

5.5.2 Contingency Planning Responsibility

County IT is responsible for contingency planning and for providing technical guidance for all Information Security contingency plans.

5.5.3 Periodic Testing

Oneida County IT shall periodically test the County's Information technology contingency plan(s).

5.6 Acceptable and Unacceptable Use Policy

5.6.1 Acceptable Use

Users are responsible for exercising good judgment regarding the use of the County's Information Resources. The County's computers or networks shall not be used for personal or commercial use or to facilitate unethical or criminal activities. The County's computers and networks are only to be used for official County business.

Communications by Users from a County e-mail address must contain the following disclaimer:

This e-mail, including any attachments, may be confidential, privileged or otherwise legally protected. It is intended only for the addressee. If you receive this e-mail in error or from someone who was not authorized to send it to you, do not disseminate, copy or otherwise use this e-mail or its attachments. Please notify the sender immediately by reply e-mail and delete this e-mail from your system.

5.6.2 Unacceptable Use

Under no circumstances are Users authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing County-owned resources.

Users as employees, interns and temporary workers, found to be in violation of this Policy may face disciplinary actions including employment termination as well as civil and criminal liability. The Department Head or his designee shall be responsible for ensuring all Users as an employee, intern or temporary workers, contractors and/or vendors, for whom they have control or authority over shall comply with the provisions of this Policy.

Nothing contained in this Policy in intended to supersede the rights, and/or disciplinary procedures in a User employee's collective bargaining agreement.

Users as vendors and/or contractors shall be held accountable for unacceptable use of County owned resources. The County shall pursue all legal remedies available to it in law, against any User as a vendor and/or contractor for any violation of this policy. The listings below are by no means exhaustive due to the constant change in IT, but attempts to provide a framework for activities thatfall into the category of unacceptable use.

5.6.2.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the County;
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music or movies, and the installation of any copyrighted software for which the County does not have an active license is strictly prohibited;
3. Exporting software, technical information, encryption software or technology, in violation of international or national export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question;
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to anyone or allowing use of your account by others. This includes supervisors, IT, vendors as well as family and other household members when work is being done at home;
6. Using a County computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws;
7. Making statements about warranty, expressly or implied, unless it is a part of normal job duties;
8. Effecting security breaches or Disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the User is not expressly authorized to access, unless these actions are within the scope of regular duties. Examples:
    a. Interfering with or denying service to any user other than the User's host (for example, denial of service attack);
    b. Using any program/script/command or sending messages of any kind with the intent to interfere with or disable a user's terminal session via any means locally or via the Internet/Intranet/extranet;
9. Port scanning or security scanning is expressly prohibited unless performed by authorized IT staff as required to perform regular job duties;
10. Executing any form of network monitoring which will intercept Data not intended for the User's host, unless this activity is a part of the User's normal job/duty (e.g., IT staff);
11. Circumventing User Authentication or security of any host, network or account;

12. Providing information about or lists of County staff to parties outside County government, unless the information is considered public;
13. Using encryption on County Information Systems without providing the encryption keys to IT;
14. Intentionally changing hardware and software configurations as deployed by IT without written authorization from the County Executive or County IT.

5.6.2.2 Email and Communications Activities

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) unless permission is granted by the County Executive;
2. Unauthorized use or forging of email header information (a.k.a. e-mail spoofing);
3. Solicitation of e-mail for any other email address, other than that of the poster's account,with the intent to harass or to collect replies;
4. Creating or forwarding "chain letters," or other "pyramid" schemes of any type;
5. Violate any guidelines for behavior set forth in the Oneida County Personnel Rules, the Oneida County Code of Ethics and the Collective Bargaining Agreement in effect for their Union when using email and other County communication resources. Users shall comply with the County's Social Media Policy.

5.6.2.3 Web Servers, MUDs, Network Games, Listservs, Other Computer Applications on County Information Systems

Users may not have web servers, Multi-User Dungeons (MUDs), network games, unauthorized computer applications, file sharing programs or file transfer programs (e.g., Napster, Gnutella, Kazaa, Morpheus, Audiogalaxy, BearShare, LimeWire, imesh, WiniN4X, Madster, etc.) or listservs running on County information systems without written consent from the CISO.

5.6.2.4 Security Circumvention

Users must not attempt to compromise information system security measures in any way. Incidents involving unapproved system hacking or cracking, password, file decryption or similar attempts to compromise security measures will be considered violation of this Policy. Unless specifically authorized by the CISO, in consultation with the County Executive, Users, including IT staff, must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or

compromise the County's information systems security. Users, including IT staff, found in violation may face disciplinary measures, which may include immediate dismissal.

5.7 Privacy Expectations for Users

Users should have no expectation of privacy when using County IT network, equipment or services including but not limited to mobile devices, PCs, servers, Intranet or Internet connections. Users should be aware that Internet/Intranet/extranet related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing and FTP are the property of Oneida County Government and **thus Users have NO expectation of privacy**. The County reserves the right to access, inspect and monitor all messages and files on the County's network, servers, mobile devices, laptops or workstations and user access to the internet as deemed necessary and appropriate.

Backup copies of e-mail and Data files are maintained and may be reviewed by authorized individuals for legal, business or other reasons.

Monitoring will be performed by authorized County personnel and vendors that support monitoring systems in use by County IT. Those authorized to do so may monitor and log usage Data, review this Data for evidence of violation of law or County policy, and may monitor all the activities and inspect the files and messages of specific Users of County computers and networks. All communications including audio, text and images can be disclosed to law enforcement or third parties without prior consent of the sender or receiver.

5.8 County Information Security Audit Policy

The County CISO has the authority to conduct a security audit on any County Information System. Audits may be conducted to:

1. Ensure integrity, confidentiality and availability of information and resources;
2. Investigate possible security incidents;
3. Ensure conformance to the County's security policies;
4. Monitor user or system activity where appropriate.

For the purpose of performing an audit, any access needed will be provided to members of the audit team. This access may include and is not limited to:

1. User level and/or system level access to any computing or communications device;

2. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on County equipment or premises;
3. Access to work areas (offices, desks, cubicles, storage areas, etc.);
4. Access to interactively monitor and log traffic on County networks.

5.9 Security Tools

The CISO is authorized to acquire and employ the appropriate security tools necessary to ensure confidentiality, integrity and availability of the County's information system resources. Possession or use of security tools by other than specifically authorized IT staff is prohibited. Users found in violation may face disciplinary measures, which may include dismissal.

5.9.1 Information Technology Staff Permission to Use Security Tools

IT staff, who in their job duties will require the use of Information Security tools (a.k.a. hacking tools), must obtain permission from their immediate supervisor and from the County CISO before such tools are acquired and used on the County's information resources. Additionally, the CISO may grant access and use of such appliances to the County's cybersecurity vendor to enhance security testing and monitoring.

5.10 Copyright and Licenses

Failure of Users to observe copyright or license agreements may result in disciplinary action or legal action by the copyright owner and by the County. Users will be held personally liable for intentional and/or reckless violations of the copyright laws and license agreements. Supervisors will also be held personally liable if they intentionally and/or recklessly violate copyright laws and/or license agreement and did not take any action to correct and to prevent copyright and licensing violations. Violations by Users will be referred to the Personnel Commissioner and the County Attorney for appropriate action.

5.11 Disclosure of Information System Vulnerabilities

System Vulnerabilities and security Incidents must be handled on a need-to-know basis. Also, security analyses of the County's Information Systems security posture are to be considered confidential information to be handled on a need-to-know basis. The CISO will place all hardcopy or electronic documents, notes, memos on investigative results, in a secured file to which only the County Executive, County Attorney, the County's Cybersecurity Team, and the CISO have access.

5.12 Reporting Suspected Security Incidents / Violations

It is every user's responsibility to immediately report, in confidence, all suspected policy violations, suspected system intrusions or other conditions that might jeopardize the County's information security to their supervisor, Department Head, County Executive, or CISO.

5.13 Violations

5.13.1 Non-Compliance

All Users are required to comply with all the measures outlined in this policy. Violations of the provisions of this Policy may lead to disciplinary action including termination and criminal prosecution.

5.13.2 Disciplinary Review

Violations will be dealt with according to current employee disciplinary practices.

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 may be applied.

5.13.3 Absence of Guidelines

The absence of specific guidance covering a particular situation does not relieve Users from exercising the highest ethical standard applicable to the circumstances. When in doubt Users should contact their immediate supervisor, Department Head, CISO or the County Executive.

6 PART II: Technical Policy

6.1 The County's Information Systems Connections

6.1.1 External Connections

Oneida County IT must approve all external connections before any external connection is made and all connections must adhere to policies and procedures for security as set forth by the applicable

County Management. All entities, meaning County departments connected to the County network are required to maintain an up-to-date list of all external connections in use, and to provide the list to Oneida County IT. Non-compliance in maintaining such a list or not providing the list to IT allows it to terminate any connection to the County Network so as to preserve a secure environment. The CISO is granted the authority to direct staff to remove connection points on the County's network under the CISO's control that pose a security risk to the County network.

The intent of this Policy is to ensure that those responsible for the security of the County's network are aware of all external connections. Unless these connections are known, they cannot be secured. Any unsecured external connection can lead to security compromise of the entire County network.

The County's cybersecurity vendor utilizes security appliances and applications at the discretion of the CISO in order to monitor for any unauthorized connections to the County network as an additional layer of security against unauthorized access.

6.1.2 Modems

The use of modems on the Oneida County WAN or on any LAN connected to the WAN is not allowed. If a business reason exists for a modem to be used, a business case must be presented to the CISO. Only the Oneida County CISO has the authority to approve the use of a modem connection. Any approved modem connection shall be in accordance to the security policies and procedures set forth by IT for such connections.

This Policy eliminates security vulnerabilities created by dial-up connections using modems. Modems are considered a weak link in security. For example, Users may install a modem on their computers so they can access the Internet through their personal Internet Service Provider and, atthe same time, they are connected to a County LAN, and thus they are accessing the Internet in a manner that bypasses all County perimeter security—allowing a direct connection to the Internet.

6.1.3 Remote Access to the County's Network by Users

Remote access to the County WAN by the Users shall only be via methods that ensure the security of the County's network and are approved by the CISO. Only the County Executive or the CISO have the authority to grant Users remote access to the County's network, and only after reviewing with the Department Head the need for such access and access requirements.

6.1.4 Wireless

Wireless access points/base stations connected to County networks must be approved and registered by Oneida County IT. "Peer-to-peer" wireless connections are not permitted.

Connecting County-owned equipment to non-County wireless access points without prior approval by Oneida County IT is prohibited.

6.1.5 Wireless Routers

Wireless routers that allow computers, smartphones or other devices to connect to the Internet or to communicate with one another wirelessly within any Oneida County facility are not allowed unless authorized by the Department Head and the CISO.

6.1.6 Home Personal Computers

Home personal computers are considered non-secure devices. County Data is not to be stored on an employee's home personal computer.

If a home personal computer uses a Virtual Private Network (VPN) to access County Data, then: 1) employee must receive approval from their Department Head and IT Department to use the VPN to access County Data; and 2) employee is responsible for demonstrating to County IT that a home personal computer complies with all the requirements set forth in this document.

Accessing PHI using a home personal computer is prohibited.

6.1.7 Third Party Access

Before any third party, in some instances a User as a contractor and/or vendor may be considered a third party, is allowed to connect to the County WAN, a third party connection agreement must be executed between the County and the third party. The CISO, and County Executive are the final approval authority for such agreements. The agreement at a minimum shall outline the third party's responsibilities. The third party shall hold harmless and indemnify the County for any breach of the agreement and this Policy. The terms of this Policy shall be incorporated by reference into the agreement. The agreement shall comply with Section 2202 of the Oneida County Charter, and shall be executed with the formalities stated therein.

6.1.8 Inter-Municipal Agreements

Before any municipality is allowed to connect to the County WAN, an Inter-Municipal agreement must be executed between the County and the municipality. The County Executive is the final approval authority of such agreements.

The agreement at a minimum shall outline the municipalities' responsibilities. The municipality shall hold harmless and indemnify the County for any breach of the agreement and this Policy. The terms of this Policy shall be incorporated by reference into the agreement. The agreement shall comply with Section 2202 of the Oneida County Charter, and shall be executed with the formalities stated therein.

6.2 System Privileges/Access

County IT staff will have elevated system privileges and system access to the extent necessary to effectively perform their jobs.

6.2.1 Granting System Privileges

Requests for changed user privileges must be in writing and approved by the Department Head and submitted to IT before the request is fulfilled.

6.2.2 Inactive Accounts

Accounts shall be established to deactivate if the account has been inactive for thirty (30) calendar days.

6.2.3 Need-to-Know

The Information System privileges of all Users are to be restricted based on a "need-to-know" Basis. This means that privileges on County Information Systems must not be extended unless a legitimate business need for such privileges exists. The intent of this Policy statement is to limit access to the County's Information so that Users do not to have privileges beyond those necessary to perform their job function.

6.2.4 Group or Shared Accounts Prohibited

Information Systems access control and audit ability shall be achieved via the use of user accounts that are unique to each individual user. Access control to files, applications, databases, computers, networks, and other system resources via shared accounts (user ids) (also called "group accounts") and shared passwords (also called "group passwords") are prohibited.

6.2.5 Guest and Anonymous User-Ids

Anonymous and "guest" user-IDs are prohibited.

6.2.6 Revoking System Access

6.2.6.1 User Status Change

Department Heads must promptly report all significant changes in Users' duties that are under their supervision, as it relates to their need for Information access. Network Administrators must promptly revoke privileges no longer needed by a User. The County shall have a process in place by which changes in a User's duties as they relate to Information and network access are communicated to IT.

6.2.6.2 County User Departure (Voluntary or Termination)

In the event a User leaves County service, the County shall ensure that the User's access to County Information resources is disabled. The Department Head shall promptly notify County IT of all User separations (e.g. Employees, temps, contractors, etc.) and, in turn, IT shall promptly disable the User's account and access to the County's Information Systems and Information. As soon as a separation date is identified, it will be the responsibility of the Department Head to direct IT regarding how to handle the former User's email and network drives. Options include having IT post an autoreply to email received into the former user's mailbox and moving files from the former User's network drive to another user drive. Auto-replies to email will be left in place for up to six (6) months at which time the email account will be deleted.

6.2.6.3 Authorization to Revoke User Access

Authorization to revoke a County Employee's access to all County Information resources and accounts will be according to the following chart:

Group:	Authorized By:
User (Not Department Head, Elected or Appointed Official)	Head of the Department the user reports to
Department Head	County Executive
County Executive	Chairman of the Legislature
Elected Official	Chairman of the Legislature

6.2.7 User as Contractor/Vendor's Access Privileges

Vendors must not have access privileges by default to the County's Information Systems. Vendors needing to provide maintenance on equipment via remote access must coordinate withthe CISO or his/her designee. All vendor activity will be closely monitored and logged by IT. All Vendors will be required to read and sign the Oneida County Acceptable Use Policy agreeing to abideby the intent of this Policy prior to being given access to the County Network.

6.2.8 Screen Savers

Users are required to have password protected screen savers activated. After 10 minutes of no activity, the screen saver blanks the screen. The user will need to re-authenticate to resume work.

6.2.9 Protecting Sensitive Information

If the Information access by the User on a computer is Classified as PHI, HIPAA or is highly Confidential, Users must not leave their workstation without first logging-off the network, locking their PC or enabling a screen saver requiring re-Authentication to continue work.

6.3 Log-In / Log-off Process

6.3.1 Network Log-in Banner Required

Every County System, where technically feasible, shall employ a log-in banner that includes a warning notice. This notice must state:

- the system is to be used only by authorized County Users;
- by continuing to use the system, the user acknowledges that he/she is an authorized User; and
- the User consents to monitoring.

The use of a log-in banner is required to warn a potential user that only authorized Users are allowed access, and they are responsible for their use of the County's Information Systems. In addition, Users are put on notice that their actions may be monitored and consent to the monitoring.

6.3.2 User Authentication Required

At a minimum, positive identification for login into County Information Systems involves both a user-ID and a password, both of which are unique to an individual user. Other additional methods of Authentication (e.g., token-based, smartcard, biometric) will be used where appropriate.

6.3.3 Log-in Prompts

The login process for the County's Information Systems and applications must simply ask the User to log-in providing prompts as needed. Specific information about the County, the computer operating system, or the network configuration must not be provided until a User has successfully been authenticated.

If any part of the login sequence is incorrect, the person logging in must not be given specific feedback indicating the source of the problem - whether it was due to an invalid user-ID or to an invalid password. Instead, the person logging in must simply be informed that the login processwas incorrect.

6.4 Password Policy

6.4.1 Initial Password Set-up

Wherever system software permits, the initial passwords issued to a new user must be valid only for the user's first login. At the first-login, the user will be forced to set a new password. This same process applies to the resetting of passwords in the event that a user forgets a password.

6.4.2 User as Contractor/ Vendor-Supplied Default Passwords

All vendor-supplied default passwords on software and hardware must be changed before any software or hardware is made operational on the County's information systems.

Hardware and software comes with default accounts and passwords used by vendors for various reasons (e.g., diagnostic, testing). These default accounts and passwords are usually publicly known, and thus need to be disabled or changed before the software or hardware is installed on the County's network.

6.4.3 Security Compromised

Whenever the security of the Information System has been compromised, or if there is a convincing reason to believe that the Information System has been compromised, the involved Network Administrator must immediately force every password on the involved system to be changed at the next login. If systems software does not allow for that, the Network Administrator shall broadcast a message to all Users informing them of the required actions. If the situation warrants, the Network Administrator must immediately reset all passwords on the affected systems. At the discretion of the CISO and depending on the nature of the compromise, the County's cybersecurity vendor may be notified.

6.4.4 Accountability

Users are accountable for all usage of their County provided accounts, and therefore shall not grant access to their account to any person or entity. The assumption by the County is that only the authorized user of an account has access to it. Therefore, the authorized user is accountable for all actions associated with the account. This maintains the audit ability of user actions, so the Users cannot claim that someone else used their account to take unauthorized actions.

6.4.5 Password Disclosure

Users must never disclose their password(s) to anyone (including a superior or IT) or to any entity under any circumstances.

If access to certain County resources is required for business purposes, the Department Head should approve the access. Under no circumstances should any user provide access to said resources via sharing a password or through other means. If a password is unintentionally disclosed or suspected of being compromised, the user shall immediately change the password and notify the CISO.

6.4.6 Positive Identification to Reset Password

To obtain a new or changed password, the Network Administrator must positively authenticate the identity of the person making the request. Only upon positively identifying the person will the Network Administrator reset a password.

6.4.7 Password Selection

The first line of defense to prevent an attack against the County's Information Systems is the use of passwords that meet certain complexity requirements. Users are to choose a password that meets the following minimum complexity requirements:

1. Minimum length is 14 characters

2. Must contain at least one number (1, 2, 3, 4 ...)
3. Must contain at least one capital letter (A, B, C, D …)
4. Must contain at least one lower case letter (a, b, c, d …)
5. Must contain at least one symbol ($, !, # …)
6. Must not contain the user account name (will also be rejected for partial account name)
7. Must NOT be written down

6.4.8 Password Aging

All Users shall be forced by the network to change their passwords at least once every ninety (90) days.

6.4.9 Tracking Previous Passwords Used

If system software permits, a history file of passwords must be employed to prevent Users from reusing passwords. The history file must minimally contain the last twenty-four (24) passwords foreach user-ID.

6.4.10 Password Storage

For all County Information Systems, passwords must be encrypted when stored or transmitted. Passwords must not be stored in unencrypted form in batch files, automatic login scripts, software macros, terminal function keys, computers without access control systems, or in other locations where unauthorized Users might discover them. Similarly, passwords must not be written or produced in hard copy form and left in a place (e.g., a post-it note under the keyboard, next to the monitor screen or inside the laptop or iPad cover) where unauthorized Users might discover them.

6.4.11 Limited Number of Log-in Attempts

Access to an account will be locked-out if an unreasonable number of unsuccessful login attempts occur during a preset time period. A maximum of 3 failed login attempts will be allowed before the account is locked-out. The user is required to contact IT in order to regain access to their account. IT will take appropriate precautions to positively identify the user before re-enabling access to the account. The Department Head may be contacted to positively identify locked out Users.

6.5 Information Systems Backup

6.5.1 Backup Responsibility

To protect the County's Information resources from loss or damage, IT is responsible for the installation of automated back-up hardware and/or software. All critical information must be backed up on a regular basis. Information shall be backed up on the County network on a nightly, weekly, month-end and annual basis.

6.5.2 Backup Plan

County IT shall formulate a backup plan for all County Information resources. Regular backups of all the Information is required as part of risk mitigation and contingency planning. In case of a security breach or loss of Data, backup files may be used for recovery purposes.

6.5.3 Backup Testing

All backups of critical data must be tested periodically to ensure that they still support full System recovery. Network Administrators or Information custodians must document all restore procedures and test them at least annually. Backup media must be retrievable 365 days a year.

6.5.4 Offsite Storage of Backups

The backup itself must be carefully protected. A copy of the backup will be made and stored offsite (out of the building). The offsite storage location must provide evidence of adequate fire and theft protection and environmental controls.

6.6 System Logs

6.6.1 System Logs Enabled

All County Information Systems shall log security events. Examples of significant security events includes Users switching user IDs during an on-line session, attempts to use passwords, attempts to use privileges that have not been authorized, modifications to system software, changes to user privileges, and changes to logging subsystems. The CISO is responsible for dictating the monitoring and review of security logs and may leverage the County’s cybersecurity vendor.

6.6.2 Accountability and Traceability for All Privileged System Commands

All special privileged commands issued on the County's Information Systems must be traceable to individuals via comprehensive logs.

6.6.3 Reviewing Logs in a Timely Manner

To allow proper action to be taken in a timely manner, security event logs must be reviewed in a timely manner.

The frequency of the review is dependent on the Sensitivity of the Information and the criticality of the System. Each Department Head and custodian will need to determine the appropriate period for reviews. The CISO works in conjunction with the County's cybersecurity vendor to monitor security appliances and review logs as appropriate.

6.6.4 Clock Synchronization

All computers and multi-user systems connected to the County WAN must always have its internal clock synchronized with a master clock for purposes of correlating significant security events.

6.7 Malicious Code

6.7.1 Malicious Code Detection

The County shall employ the use of Malicious Code detection software on all its Systems. Malicious Code checking programs are to be kept current via automated means.

The County's SOC monitoring team is responsible for ensuring all malicious code that is detected is investigated commensurate with the threat level to County systems. Managing of malicious code is completed at the discretion and under the supervision of the CISO.

6.7.2 Protecting Mobile Computing Devices from Malicious Code

County IT shall develop a process for Users using mobile computing devices (e.g., laptop computers) to receive timely updates to the software used to protect against Malicious Code (e.g., viruses). Users

have the responsibility to ensure that their mobile computing device has the latest protection against Malicious Code by following the policies and procedures set forth by IT.

6.7.3 Initial Scanning of Software

Software on all County systems must be scanned for malicious code and copied or backed up prior to its initial use. The copies must not be used for ordinary business activities but must be reserved for recovery from malicious code infestations and other security problems.

6.7.4 Malicious Code Eradication

Users are prohibited from attempting to eradicate Malicious Code from a system on the County's Information System unless they do so in conjunction with authorized IT staff. If a virus or other malicious code is detected, IT is to be notified immediately. The computer is not to be shut down but will be removed from the network by IT upon discovery.

6.8 Mobile Devices

This section applies to laptop computers, Handheld Computers, tablets, smart phones, and Mobile Storage Devices such as USB flash drives or memory sticks, CDs, DVDs, diskettes, MP3 players, digital pens etc., that are used for storing data. Mobile devices are subject to safeguards to protect the Confidentiality of the Data on them. The guidelines below outline the steps needed to ensure the proper use and administration of mobile devices.

1. All mobile devices that receive County Information (e.g. County email) or contain County Information (e.g. pictures) must be registered with IT. This includes all personally owned and County owned devices.

2. Any mobile device should be used only by the individual that has registered it. Any mobile device should not be used by any other individual outside of County government.

3. Mobile devices and media must be password protected.

4. Any mobile device or media should protect the data with a method of Data Encryption. Exceptions may be made by the CISO in conjunction with Department Heads. A record of the exceptions will be kept on the Mobile Device Inventory.

5. Wireless data transmission to and from the mobile device, including syncing, must be done via an encrypted connection.

6. Mobile devices should be safeguarded from theft or loss the same way as a personal credit card.

7. All mobile devices will indicate method of return to IT Department if found. Any misplaced mobile device must be immediately reported to the CISO.

8. All mobile devices are subject to the same security guidelines as workstation units including restricting visibility of display in public areas.

9. All data contained on mobile devices must be backed up on a regular basis according to the policies and procedures set forth by IT.

10. Mobile Media that leaves the County worksite must follow all mobile device requirements.

11. Mobile devices are to be synchronized only to a County-approved computer.

12. Disposal of any mobile device must follow the guidelines set forth in the Oneida County Procedures for Protecting PPSI When Disposing or Reusing Electronic Equipment.

13. Laptop computers shall be encrypted to protect Sensitive Information that may be resident on the device.

6.9 Encryption

6.9.1 Use of Encryption

Use of Encryption on the County's Information System will only be done using processes approved by the CISO, and only for official County business. Users are forbidden to use Encryption for any other purposes except for official County business.

6.9.2 Transmittal of Sensitive Information

Sensitive Information that is to be transmitted outside the County's WAN or via email or the Internet shall be Encrypted. The requirement for Encryption is set by the applicable Department Head. Oneida County IT sets and the CISO approves the Encryption processes to be used by the County to meet this requirement.

6.9.3 Storage of Sensitive Information

Sensitive Information stored on County Information Systems must be Encrypted. In addition, any archived (back-up copies) Sensitive Information also needs to be Encrypted.

Encrypting stored Sensitive Information adds another security layer to the defense in depth concept. Encryption archived Information prevents someone with access to the back-up tapes to access

Sensitive Information.

6.9.4 Encryption Keys

Encryption keys used by the County shall be treated as confidential information. Access to Encryption keys shall be strictly limited to those who have a need-to-know basis.

6.9.4.1 Encryption Key Escrow

Copies of all Encryption keys will be kept in escrow and accessible by the County Executive and CISO.

6.10 Transfer of Computer Equipment and Media

6.10.1 Internal to the County

The County strives strongly to protect the confidentiality of Information entrusted to it. As the County upgrades computing equipment, equipment may be moved to other areas within the County. To protect Information entrusted to the County, the proper measures need to be employed to ensure that all data is removed from the computer's storage media before the computer is relocated to another location within the County. The removal of such data shall be conducted by IT using methods including but not limited to reimaging as approved by the CISO that ensure that any previously stored Information will not be recoverable.

6.10.2 Outside the County

As the County upgrades its computer systems, the County may decide to dispose of its old computers. Before any computer is approved as surplus and leaves County premises, IT shall be contacted and shall ensure that the hard drive is removed and drilled ensuring that any previously stored Information on the media is not recoverable. Removing data by methods other than drilling the hard drive will be considered on a case-by-case basis and must be approved by the CISO.

6.11 Hardware and Software Configuration

Configurations and set-up parameters, as defined by Oneida County IT for deployed hardware and software must comply with County security policies and procedures. The configurations and parameters have been designed with security in mind as well as the County's ability to conduct business. Any changes in the configurations and set-up parameters of deployed hardware and software

can undermine overall security, and thus are **forbidden,** unless approved in advance by the CISO. IT reserves the right to disconnect from the County network any hardware or software application with configuration or parameters that are not compliant.

6.12 Physical Security

Physical access to wiring closets and computer machine rooms, and the like, must be restricted to authorized personnel only. The equipment must be located in locked rooms or inside locked cagesto prevent tampering and unauthorized use. Information technology equipment must be protected from power surges, power failures, water damage, overheating, fire, and other physical threats.

6.13 Systems Development and Maintenance

Security requirements and controls must reflect the business value of the Information involved and the potential business damage that might result from a failure or absence of security controls. It is required that security requirements be considered throughout the systems development life cycle (SDLC). Whenever new systems are procured or developed or existing systems significantly modified by either in-house or vendor personnel, the procedures developed by the CISO in conjunction with all applicable parties shall be followed.

Appendix A: SECURITY OFFICIAL JOB DESCRIPTION

Title: Chief Information Security Official (CISO)

Reports to: County Executive

Overview: The CISO is the individual responsible for Oneida County's on-going Information Security program. This includes all activities related to developing, implementing and maintaining security-related policies and procedures and monitoring performance to ensure that the confidentiality, integrity and availability of ePHI is adequately protected. The CISO is expected to help management create an environment in Oneida County that reinforces the importance of securing ePHI. This may be a part time or full time position depending on need.

Responsibilities:

1. Serves as the County's internal resource for all security-related matters, coordinating activities between departments and offices as needed.

2. Supports Oneida County's workforce and management in implementing sound security practices and preventing security incidents.

3. Prepares security policies, procedures, and supporting material in accordance with applicable regulations and commonly accepted security and risk management practices, and recommends updates as required by operational, environmental, technological or regulatory changes.

4. Directs departments in performing initial and periodic assessments of the County's Information Security risks and proposes cost-effective security measures to ensure that ePHI is adequately protected and that Oneida County remains in compliance with HIPAA Security Rule requirements.

5. Promptly investigates security Incidents brought to their attention and pursues resolution in conjunction with department management as needed.

6. Regularly reviews system activity data and reports to management on the status and effectiveness of the County's Information Security efforts.

7. Cooperates with federal and state officials and other legal entities and organizations in conducting compliance reviews of investigations.

8. Facilitates Oneida County's security awareness and training efforts and ensures that workforce training is conducted as required.

9. Maintains required security documentation, including security Incident logs, Risk Assessment and Risk Management documents, policies and procedures and records of any sanction actions.

10. Works with Oneida County's privacy officials to ensure successful implementation of the County's HIPAA compliance programs.

Qualifications:

1. Knowledge of current federal and state Information Security laws and regulations as they pertain to safeguarding PII and ePHI.

2. Familiarity with Oneida County's operations and Information Systems and other computerapplications utilized to support those operations.

3. Familiarity with commonly accepted security and Risk Management practices.

4. Familiarity with technical tools utilized to secure ePHI and monitor Information System performance.

5. Ability to propose and implement cost effective security measures appropriate to the County's operations

6. High degree of personal integrity and trust

7. Skill working with personnel at all organizational levels

8. Analytical, written and verbal skills

Responsibilities of Members of the County's SOC Monitoring Team

1. Implement sound security practices to prevent security Incidents.
2. Prepare security policies, procedures, and supporting material in accordance with applicable regulations and commonly accepted security and Risk Management practices, and recommend updates as required by operational, environmental, technological or regulatory changes.
3. Facilitate departments' initial and periodic assessments of their Information Security risks and implement cost-effective security measures, based on the advice of the CISO, to ensure that ePHI is adequately protected and that departments covered by HIPAA regulations remain in compliance with HIPAA Security Rule requirements.
4. Assist the CISO in promptly investigating security Incidents brought to their attention and pursuing resolution in conjunction with the CISO as needed.
5. Implement the County's security awareness and training and ensure that workforce training is conducted in all departments as required.
6. Ensure proper contracts and agreements are in place with Business Associates (under HIPAA regulations) and other entities as required by law or regulation.
7. Make other people and agencies, such as business associates, aware of the County's security practices.

Appendix B: Glossary

Authentication: The process to establish and prove the validity of a claimed identity.

Availability: This is the 'property' of being operational, accessible, functional and usable upon demand by an authorized entity, e.g., a system or a user.

Breach: Unauthorized acquisition of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the County.

Classification: The designation given to information or a document from a defined category on the basis of its Sensitivity.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls: Measures employed to satisfy the requirements set forth in this policy.

County Entity: County Entity, for the purposes of this policy, shall include all County departments, offices, etc. over which the County Executive has executive power.

Custodian: An employee or organizational unit acting as a caretaker of an automated file or database on behalf of a department.

Data: Data shall be defined as any information created, stored (in temporary or permanent form), produced or reproduced, regardless of the form of media. Data, in both electronic or hard copy form, may include, but is not limited to, personally identifying information, reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

Disaster: A condition in which information is unavailable, as a result of a natural or man-made occurrence that is of sufficient duration to cause significant Disruption in the accomplishment of the County's business objectives as determined by the County leaders.

Disruption: Activities such as network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

Encryption: Rendering data unintelligible to anyone without a password.

ePHI: (electronic protected health information) Information that is defined as "protected health information" under HIPAA.

Extranet: A private network that uses Internet technology and the public telecommunications system to securely share information or operations with any non-County entity

Handheld Computer: Small computer running mobile version of operating system.

HIPAA: The Health Insurance Portability and Accountability Act of 1996. This act affects the confidentiality and security practices of several departments within the County including Department of Social Services, Mental Health Department, and the Health Department.

Incident: Any adverse event in an information system or network or the threat of the occurrence of such event.

Incident Response: The manual and automated procedures used to respond to reported network intrusions (real or suspected), network failures and errors, and other undesirable events.

Information: Information is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means.

Information Assets: (1) All categories of automated information, including but not limited to: records, files, and databases, and (2) information technology facilities, hardware and software owned or leased by the County.

Information Security: The concepts, techniques and measures used to protect information from accidental or intentional unauthorized access, modification, destruction, disclosure or inability to process the information -- be it temporary or permanent.

Information System: An interconnected set of information resources under the same direct management control that shares common functionality. A system may include hardware, software, information, data, applications, or communications infrastructure.

Integrity: The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.

Internet: A system of linked computer networks, international in scope, that facilitates data transmission and exchange, which uses the standard Internet protocol, TCP/IP, to communicate and share data.

Intranet: The intranet is an internal (i.e., non-public) network that uses the same technology and protocols as the Internet.

Intrusion Detection: The monitoring of network activities, primarily through automated measures, to detect, log and report actual or suspected unauthorized access and events for investigation and resolution.

IT: Information Technology. (Usually refers to Oneida County IT.)

LAN: Local Area Network

Laptop Computer: Mobile computer running standard operating system.

Malicious Code: Programming or files that are developed for the purpose of doing harm and exploiting data security, examples of which are viruses, worms, Trojan horses, spyware, and phishing.

Non-Repudiation: Non-repudiation is the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified.

Off-site Backup: Mechanism to backup or archive PHI in a physical location other than that in which the data is primarily stored.

Owner: The department responsible for maintaining the integrity of the data.

PHI: Protected Health Information. A HIPAA term for any information (such as name, address, photo, diagnosis, etc.) used in a health-related context that should be kept confidential.

Mobile Media: Floppy Disk, CDROM, DVD, USB Hard Drive or other media designed to store data.

Mobile Storage Device: Device used for storing data such as USB flash drives or memory sticks, CDs, DVDs, diskettes, MP3 players, digital pens etc.

Procedures: Specific operational steps that individuals must take to achieve goals stated in policy.

Private Information : Personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number; or

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password, which would permitaccess to an individual's financial account.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Risk: The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome.

Risk Assessment: The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.

Risk Management: The process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

Sensitivity: The potentially harmful impact resulting from disclosure, modification, or destructionof information.

SO: CISO—appointed by the County Executive; see job description.

Threat: A threat is a force, organization, or person which seeks to gain access to, or compromise, information. A threat can be assessed in terms of the probability of an attack. Looking at the nature of the threat, its capability and resources, one can assess it and determine the likelihood of occurrence, as in Risk Assessment.

Trojan Horse: Is a program in which malicious or harmful code is contained inside an apparently harmless program and, when executed, performs some unauthorized and undesirable activity or function.

User: Any person, organizational entity, or automated process that accesses a County system for legitimate government purpose, as authorized by the County of Oneida, including but not limited to employees, contractors/vendors, consultants, temporaries, all personnel affiliated with third parties and other workers at Oneida County.

Virtual Private Network (VPN): Is a way to use a public infrastructure, such as the Internet, to provide remote offices or individual Users with secure access to their organization's network.

Virus: A malicious program that replicates itself on computer systems by incorporating itself into other programs that are shared among computer systems. Once in the new host, a virus may corrupt files, display unwanted messages, crash the host, etc.

Vulnerability: A weakness of a system or facility holding information which can be exploited to gain access to violate system integrity. Vulnerability can be assessed in terms by which the attack would be successful.

WAN: Wide Area Network—a network that connects two or more LANS.

Worm: A worm is a self-replicating piece of malicious software, similar to a virus, but requires no user action to activate it. A worm exploits weaknesses in operating systems and other applications to propagate itself to other systems.