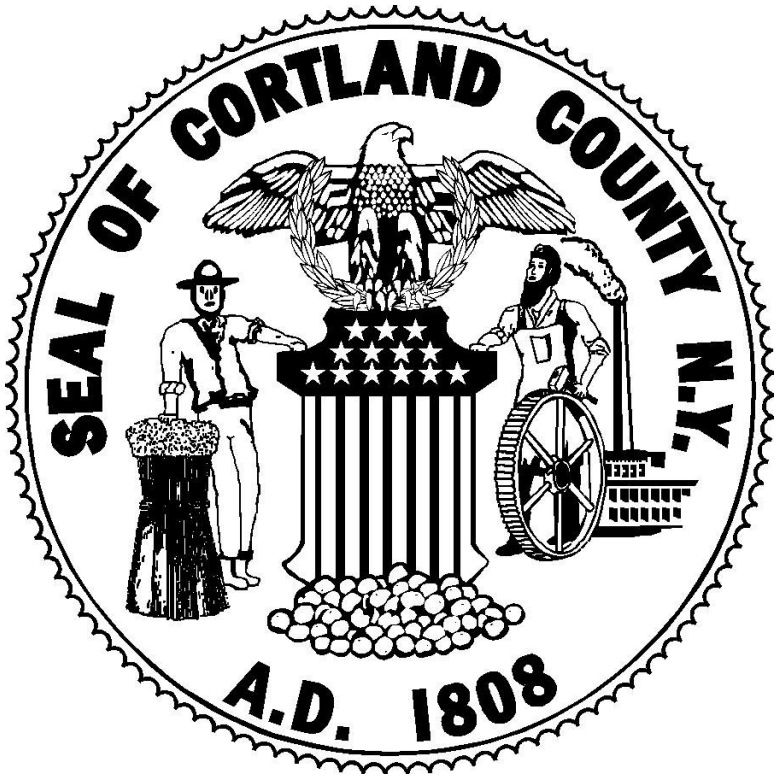
# CORTLAND COUNTY
# INFORMATION SECURITY POLICY




Release authorized by:
The Cortland County Legislature

Adopted 6/24/2010

Resolution #192-10

2010

# Cortland County Information Security Policy

**Table of Contents**

## 1. Purpose

Access to Cortland County's (hereinafter referred to as the County) information systems has been provided to all authorized County Entities[1], employees, consultants, contractors, interns, volunteers, and temporary workers (hereinafter referred to as "users") for the purpose of providing service to the residents of Cortland 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 systems in a legal/ethical manner consistent with County & 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**: This policy is effective as of the date of issuance.

- **Expiration Date**: This policy remains in effect until superseded, amended, or canceled.

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.

1. **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.

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

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

[1] County Entity, for the purposes of this policy, shall include all County departments, offices, etc.

4. **Non-Repudiation:** The availability of irrefutable proof of:
    a. the origin of data
    b. the content integrity of data, and
    c. the receipt and, optionally, the acceptance of data such that refutation of any of these is not possible.

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) be knowledgeable of acceptable County information system usage, b) understand their information security responsibilities, and c) be held accountable for their actions.

## 2. Scope

The policies contained in this document are applicable to all of the County's internal computer network (County Wide Area Network [WAN]), interconnections with systems outside the County WAN (e.g., 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 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.

## 3. Organization of the Information Security Policy

Cortland County's Information Security Policy is comprised of two parts: Managerial Policy and Technical Policy. Managerial Policy (Sections 4 through 18) discusses policy related to use, ownership, management, disclosure and processing information on the County's information system. Technical Policy (Sections 19 through 31) discusses the policy related to the technical aspects of the County's information security.

**PART I: Managerial Policy**

## 4. County Staff 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.

Three responsibility classifications **(department, custodian,** and **user)** are defined to assist users in understanding their roles and responsibilities when using the County's information systems.

**Department:** All information residing on the County's information systems belongs to a designated department. Individual departments determine the appropriate information sensitivity classification to be applied to the information. Departments are responsible for deciding which users will be permitted to access the information and the uses to which the information will be put.

**Custodian:** Information on the County's information systems must have a designated custodian. The custodian in Cortland County is usually the IT (Information Technology) Department; however, other custodians 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:

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

**User:** The user is an individual or an organization that has been authorized access to the information asset by the department. 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 and complying with the County's information security policies.

## 5. Information Technology Asset Inventory

An inventory of information systems detailing all existing hardware, software, communication links, and names of users will be maintained by IT on an ongoing basis and reviewed annually. The format will be determined by the IT Department.

## 6. County Information Security Administration

### 6.1 Centralized Responsibility for Information Security

The responsibility and authority for the County's information security is formalized in the Security Official (SO). The SO is responsible for maintaining, coordinating, and directing specific actions that maintain the confidentiality, the integrity, the availability and the non-repudiation of County information resources as specified in the Cortland County Information Security Policy document. The SO reports to the Cortland County Administrator. See Appendix A, "Security Official Job Description," for a list of the SO's responsibilities.

### 6.2 Information Services Network and Technical Support Team Responsibilities

The IT Department 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:

- Administer network, intranet, and Internet operations in a secure manner;
- 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;
- Periodically audit the operations of all technical security measures in place to ensure the measures are operating as perceived;
- Harden systems (by removing unnecessary services and patching necessary ones) before connecting them to the Internet;
- Establish an integrated disaster recovery plan (contingency plan) to include regular backups of critical County data with offsite storage. This will be established in close coordination with the Security Task Group (STG);
- 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;
- Establish and maintain effective and secure telecommunications capabilities for/with off-site facilities;
- Identify common user deficiencies and ensuring these are addressed in information security training;
- Implement a secure system of identification and authentication to control access to County information;
- Complete a periodic review of assigned computer accounts to ensure access privileges are commensurate with user needs.

### 6.3 Systems Administrator Responsibilities

Systems administrators shall become familiar with network security concerns and take proactive measures to protect the systems and data for which they are responsible. These responsibilities include, but are not limited to:

- Implement judicious access control measures;
- Install patches expeditiously to identified system exploits (vulnerabilities);
- Educate users on security issues;
- Activate the security capabilities of the server and client systems over which they have authority;
- Review logs in a timely manner;
- Other routine activities related to security.

## 6.4 Information Security Incident Response

### 6.4.1 Security Task Group (STG)

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

### 6.4.2 Incident Response Plan

All security incidents will be investigated, according to the Incident Response Procedure, to determine immediate actions needed as well as measures to secure the County's information resources from further compromise. After a security incident, the STG will implement the following list of recovery actions to bring the affected system(s) on-line and into service:

- Investigate how the incident occurred;
- Avoid escalation and further incidents;
- Assess the impact and damage of the incident;
- Recover from the incident;
- Find out who did it (if appropriate and possible);
- Take actions to prevent and/or deter the action from recurring;
- Document the incident and preserve evidence where possible, for reporting purposes and effective resolution of an incident.

The STG 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 STG should be documented in detail for future reference.

## 6.5 Annual Information Systems Planning Process Required

The STG must 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.

## 6.6 Risk Analysis, Assessment and Management

The STG shall perform a risk assessment on all applications, systems, and services to be deployed on the County's information systems. The analysis should consist of seven steps:

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;

5. classify the damage level: high, medium, low;
6. predict occurring possibility;
7. estimate the cost of implementing security controls.

Based on the Risk Analysis, the STG, under the direction of the SO, 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).

### 6.7 Accrediting Hardware and Software

The IT Department 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.

### 6.8 Configuration Control

The IT Department will employ a documented change control process to ensure that only authorized changes are made on County information systems. This change control procedure will be used for all changes to software (upgrades and patches), hardware, communications links, etc.

### 6. 9 Current Information Security Manual Required

The STG must prepare, maintain, and distribute information security manual(s) describing the County's current information security polices and procedures.

### 6.10 Amending the Information Security Policy

The Cortland County Information Security Policy shall be amended when there is a need to align policy to stay current with laws, technology, and County business practices. The STG is responsible for drafting new policy statements or amendments to policy for review by the SO. The SO shall approve amendments to policy. Once approved, the amended policy will be in effect.

## 7. User Responsibilities

Users are responsible for adhering to policy and the security 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, fax, the intranet or Internet. No abusive, profane or offensive language shall be transmitted through the County’s systems. Users who wish to express personal opinions on the Internet are not to do so on the County’s 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 of continued protection.

Users shall:

1. Protect others' privacy 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. Coordinate the connection of Personal Communications Devices (PDAs) with the County's Security Official (SO) and the Information Technology Department (IT).
7. Coordinate the connection of devices with RF (radio frequency) capabilities (e.g., wireless access points, wireless LANs) with the SO and IT.
8. Not connect a modem to a phone line while the same computer is connected to the County LAN without approval of the SO and the IT Department.
9. Use only software licensed to the County on County computers.
10. Use robust network passwords and change them as required. (Reference Section 22.7)
11. Never share ID or passwords with anyone else, including superiors and IT staff.
12. Never document passwords and put them on or near the computer (e.g., "sticky notes" under keyboards, on monitors, etc.) (Reference Section 22.7)
13. Log off or activate screensavers with password protection to protect the County's information when computers are left unattended for more than 15 minutes.
14. Never release non-public County information unless prior authorization from the department head has been obtained.
15. Not disclose sensitive County data to other County staff other than on a need-to-know basis.
16. Secure any physical copies of sensitive County data such as tapes, floppy disks, and printouts when left unattended.
17. Report indicators of virus infection and/or operational anomalies to IT personnel or SO.
18. Report all discovered security vulnerabilities and/or computer security concerns to their supervisor and the SO and the IT Department.
19. When working at home, take reasonable measures consistent with workplace procedures to safeguard access to County information resources (e.g., computers, networks, data).
20. Never use the system for:
    a) Activities unrelated to the County's mission; (See Section 10.1)
    b) Activities unrelated to official assignments and/or job responsibilities; (See Section 10.1)
    c) Any illegal purpose; (See Section 10.1)
    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.
21. When sending confidential information, all files must be encrypted and a password sent in a separate e-mail. This applies even when sending a file through a secure network (e.g., HIN, HSEN, etc.).

## 8. Information Security Training and Awareness

### 8.1 Required Security Training

All users are to be provided with sufficient information security training and support reference materials to meet their job responsibilities. For users who are new County employees, the information security training will be incorporated into the Human Resources new employee orientation program. For users who are not County employees (e.g., consultants), the SO must be consulted for the appropriate security training. In either case, the information security training must be given before the County ITS user is allowed access to and use of the County's information systems. At the conclusion of the training, each County ITS user will be required to sign a statement that they have had information security training, understood the material presented, and had the opportunity to ask questions.

### 8.2 Compliance Statement

All users are required to sign a compliance statement, before they are given access to the County's information resources, that they have read, understood, and have been given the opportunity to ask questions concerning the County's information security policy. The compliance statement shall include language as follows: "Violations of the provisions of the information security policy may lead to disciplinary action including termination and criminal prosecution. Users shall be required to sign the compliance statement. Access to County information resources shall not be granted to anyone who does not sign a compliance statement."

### 8.3 Responsibility for Security Training

The STG is responsible for providing the material and ensuring the training sessions for new users and periodic refresher security training to remind all users of their responsibility and obligations with respect to information security.

### 8.4 Information Security Awareness

The STG is responsible for developing and conducting an information security awareness program throughout the year.

## 9. Contingency Planning

### 9.1 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 contingency and disaster recovery plan, 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 information owner) who would be affected by such a disaster.

### 9.2 Contingency Planning Responsibility

The IT Department is responsible for contingency planning and for providing technical guidance for all information security contingency plans.

### 9.3 Periodic Testing

The IT Department shall periodically test the County's information technology contingency plan(s).

## 10. Acceptable and Unacceptable Use Policy

### 10.1 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.*

### 10.2 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 found to be in violation of acceptable use policies may face disciplinary actions including employment termination as well as legal liability.

The listing below is by no means exhaustive, but attempts to provide a framework for activities that fall into the category of unacceptable use.

#### 10.2.1 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 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 the IT Department according to specified procedures.
14. Intentionally changing hardware and software configurations as deployed by IT without written authorization from the County Administrator or the IT Department.

### 10.2.2 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 Administrator.
2. Any form of harassment via email, telephone or paging whether through language, frequency or size of messages.
3. Inappropriate cartoons or jokes or anything that may be construed as harassment or showing disrespect to others to include racial or ethnic slurs and gender- specific comments.
4. Unauthorized use or forging of email header information (a.k.a. e-mail spoofing).
5. 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.
6. Creating or forwarding "chain letters," or other "pyramid" schemes of any type.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

### 10.2.3 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) or listservs

running on County information systems without written consent from the SO and the IT Department Head.

### 10.2.4 Instant Messaging
Users are prohibited from using Instant Messaging (IM) on any County information resource, unless authorized in writing by the SO and the IT Department Head.

### 10.2.5 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 the County's information security policy. Unless specifically authorized by the SO in consultation with the County Administrator, 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.

## 11. Privacy Expectations for Users
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 the County and **thus users have no expectation of privacy**. The County reserves the right to access and monitor all messages and files on the County's network, PCs, laptops or workstations as deemed necessary and appropriate.

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

Monitoring will be performed by authorized County personnel. These authorized county personnel may monitor and log usage data, may 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.

## 12. County Information Security Audit Policy
The County SO has the authority to conduct a security audit on any County information system.
Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources;
- Investigate possible security incidents;
- Ensure conformance to the County's security policies;
- 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:

- User level and/or system level access to any computing or communications device;
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on County equipment or premises;
- Access to work areas (offices, cubicles, storage areas, etc.);
- Access to interactively monitor and log traffic on County networks.

## 13. Security Tools

The SO 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.

### 13.1 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 SO before such tools are acquired and used on the County's information resources.

## 14. 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 any violations of the copyright laws and license agreements. Supervisors will also be held personally liable if they knew about copyright and/or license violations and did not take any action to correct and to prevent copyright and licensing violations. Violations by users will be referred to the Personnel Office and the County Attorney for appropriate action.

## 15. 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 Security Task Group (STG) will place all hardcopy or electronic documents, notes, memos on investigative results, in a secured file to which only the STG members and the SO have access.

## 16. Reporting Suspected Security Incidents / Violations

It is the 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 Administrator, or SO.

## 17. Violations

### 17.1 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.

### 17.2 Disciplinary Review

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

### 17.3 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, the Department Head, or the SO.

## 18. Cortland County Cyber Security Citizens' Notification Policy

### 18.1 Legal Requirement

Chapter 442 of the 2005 Session Laws require the County to adopt an information security breach and notification policy. This policy is consistent with the State Technology Law, section 208 as added by Chapters 442 and 491 of the laws of 2005.

### 18.2 Policy Content

This policy requires notification to impacted New York residents and non-residents. Cortland County values the protection of private information of individuals. Cortland County is required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and this policy.

1. Cortland County, after consulting with Cyber Security and Critical Infrastructure Coordination (CSCIC) to determine the scope of the breach and restoration measures, shall notify an individual when it has been determined that there has been, or is reasonably believed to have been a compromise of private information through unauthorized disclosure.
2. A compromise of private information shall mean the unauthorized acquisition of unencrypted computerized data with private information.
3. If encrypted data is compromised along with the corresponding encryption key, the *data* shall be considered unencrypted and thus fall under the notification requirements.
4. Notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. In such case, notification will be delayed only as long as needed to determine that notification no longer compromises any investigation.
5. Cortland County will notify the affected individual. Such notice shall be directly provided to the affected persons by one of the following methods:
    a. written notice;
    b. electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification shall be kept by Cortland County;
    c. telephone notification provided that a log of each such notification is kept by Cortland County; or
    d. Substitute notice, if Cortland County demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or Cortland County does not have sufficient contact information. Substitute notice shall consist of all of the following:
        1) e-mail notice when Cortland County has an e-mail address for the subject persons;
        2) conspicuous posting of the notice on Cortland County's web site page; and
        3) notification to major statewide media.

Cortland County shall notify, CSCIC as to the timing, content and distribution of the notices and approximate number of affected persons.

6. Cortland County shall notify the Attorney General and the Consumer Protection Board, whenever notification to a New York resident is necessary, as to the timing, content and distribution of the notices and approximate number of affected persons.

7. Regardless of the method by which notice is provided, such notice shall include contact information for Cortland County making the notification and a description of the categories

of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

8. This Policy also applies to information maintained on behalf of Cortland County by a third party.

9. When more than five thousand New York residents are to be notified at one time, then Cortland County shall notify the consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. This notice, however, will be made without delaying notice to the individuals..

## PART II: Technical Policy

### 19. The County's Information Systems Connections

### 19.1 External Connections

The IT Department 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 STG. All entities 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 the IT Department. 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 SO is granted the authority to direct staff to remove connection points on the County's network under the SO'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.

### 19.2 Modems

The use of modems on the Cortland County WAN or on any LAN connected to the WAN is not allowed. If there exists a business reason for a modem to be used, a business case will need to be presented to the STG. Only the IT Department and the SO have the authority to approve the use of a modem connection. The allowed 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, at the 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.

### 19.3 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 STG. Only the County Administrator or the SO 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.

### 19.4 Wireless

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

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

### 19.5 Air Cards

Air cards are not allowed unless authorized by the Department Head and the STG.

### 19.6 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 that a home personal computer complies with all the requirements set forth in this document.

Accessing PHI using a home personal computer is not allowed.

### 19.7 Third Party Access

Before any 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 SO is the final approval authority for such agreements. The agreement will outline the third party's responsibilities and will hold them liable if they are not compliant with the agreement.

### 19.8 Intermunicipality Agreements

Before any municipality is allowed to connect to the County WAN, an intermunicipality agreement must be executed between the county and the municipality. At a minimum the agreement outlines the roles and responsibility of the County and the municipality, and the agreement of the municipality to adhere to the security policies and procedures for connecting to the County WAN. The County Administrator and the SO are the final approval authority of such agreements.

## 20. System Privileges/Access

### 20.1 Granting System Privileges

Requests for new user-IDs and changed privileges must be in writing and approved by the department head and submitted to IT before the system administrator fulfills the request.

### 20.2 Inactive Accounts

Accounts will be established to deactivate if the account has been inactive for a specified period of time (normally 30 days).

### 20.3 Need-to-Know

The information system privileges of all users, based upon the information security policy, are to be restricted based on the "need-to-know." 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 on a need-to-know basis. Users ought not to have privileges beyond those necessary to perform their job function.

### 20.4 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. The County Administrator and SO can grant a waiver to this requirement if adequate justification is provided and security measures are determined to be appropriate.

### 20.5 Guest and Anonymous User-Ids

Anonymous and “guest” user-IDs are prohibited.

### 20.6 Revoking System Access

#### 20.6.1 User Status Change

Department heads must promptly report all significant changes in users’ duties as it relates to their need for information access. System 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.

#### 20.6.2 County Staff Departure (Voluntary or Termination)

In the event a user leaves County service, the County will ensure that the employee’s access to County information resources is disabled. As part of the process, the County’s separation checklist is to be used whenever an employee leaves County service. IT shall promptly disable the user’s access to the County’s information systems and information.

#### 20.6.3 Authorization to Revoke Employee 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: |
|---|---|
| County Employee (Not Department Head, Elected or Appointed Official) | Department Head of Dept employee works in |
| Department Head (Not Elected or Appointed) | County Administrator |
| County Administrator | Chairman of the Legislature |
| Elected or Appointed Official | Chairman of the Legislature |

### 20.7 Two User-IDs Required for Privileged Information Services Users

All who have system and network administrator privileges must have at the minimum two user-IDs. One user-ID provides privileged access (e.g., root, system administrator rights) to the County's information systems. All activity associated with the privileged user-ID will be logged. The other user-ID is the privileged user's normal user-ID for the day-to-day work of a County ITS User.

### 20.8 Vendor's Access Privileges

Vendor 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 with the SO or his/her designee. All vendor activity will be closely monitored and logged by IT.

### 20.9 Screen Savers

Users are required to have password protected screen savers activated. After 15 minutes of no activity, the screen saver blanks the screen. The user will need to re-authenticate to resume work.

### 20.10 Protecting Sensitive Information

If the information access by the user on a computer is classified as HIPAA related or is highly confidential, users must not leave their workstation without first logging-off or enabling a screen saver requiring re-authentication to continue work.

## 21. Log-In / Log-off Process

### 21.1 Network Log-in Banner Required

Every County system, where technically feasible, must employ a log-in banner that includes a warning notice. This notice must state: (1) the system is to be used only by authorized County users, and (2) by continuing to use the system, the user acknowledges that he/she is an authorized user and (3) 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.

### 21.2 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) are to be considered where appropriate.

### 21.3 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 process was incorrect.

## 22. Password Policy

### 22.1 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. The initial password must follow the guidelines in section 21.7.

### 22.2 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.

### 22.3 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 system 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 system administrator shall broadcast a message to all users informing them of the required actions. If the situation warrants, the system administrator must immediately reset all passwords on the affected systems.

### 22.4 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.

### 22.5 Password Disclosure

Users must never disclose their password(s) to anyone (including a superior) 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.

### 22.6 Positive Identification to Reset Password

To obtain a new or changed password, the system administrator must positively authenticate the identity of the person making the request. Only upon positively identifying the person will the system administrator issue a new password.

### 22.7 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:

- Must be at least 8 characters in length
- Include all of the following: Uppercase letters, lowercase letters and numbers
- May not include any part of your name in the password

### 22.8 Password Aging

All users will be automatically required to change their passwords periodically -- at least once every ninety (90) days or less.

### 22.9 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 thirteen (13) passwords for each user-ID.

### 22.10 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 or next to the monitor screen) where unauthorized users might discover them.

### 22.11 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. The number of allowable failed login attempts and the length of the lockout is dependent on the criticality of the system and the sensitivity of the information.

## 23. Information Systems Backup

### 23.1 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 according to its criticality level as defined by the applicable department head. The frequency of the backup is influenced by the frequency with which the data changes and the effort required to recreate information if it is lost.

### 23.2 Backup Plan

The IT Department 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 compromise or loss of data, backup files may be used for recovery purposes. The backup plan will address full and incremental backups.

### 23.3 Backup Testing

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

### 23.4 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) as determined by the nature of the information as set forth by the department head. The offsite storage location must provide evidence of adequate fire and theft protection and environmental controls.

## 24. System Logs

### 24.1 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.

### 24.2 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.

### 24.3 Reviewing Logs in a Timely Manner

To allow proper action to be taken in a timely manner, security 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.

### 24.4 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.

## 25. Malicious Code

### 25.1 Malicious Code Detection

The County is to employ the use of malicious code detection software on all its systems. Malicious code checking programs are to be kept current via automated means.

### 25.2 Protecting Portable Computing Devices from Malicious Code

Information Services shall develop a process for users using portable 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 portable computing device has the latest protection against malicious code by following the policy and procedures set forth by IT.

### 25.3 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.

### 25.4 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.

**26. Portable Devices** (applies to laptop computers, handheld computers, PDAs which contain PHI (Protected Health Information), cell phones, and portable storage devices such as memory sticks, CDs, diskettes, MP3 players, digital pens etc.)

Portable devices are subject to safeguards to protect the confidentiality of the data. The guidelines below outline the steps needed to ensure the proper use and administration of portable devices.

1. All portable devices must be registered with IT. This includes all personally owned and County owned devices.
2. Any portable device should be used only by the individual that has registered it. Any portable device should not be used by any other individual outside the County government.
3. Access to data on portable devices and media must be protected by the use of authentication such as a password.
4. Any portable device or media should protect the data with a method of data encryption. Exceptions may be made by the Security Officer in conjunction with the STG. A record of the exceptions will be kept on the Portable Device Inventory.
5. Wireless data transmission to and from the portable device, including the syncing of PDAs, must be done via an encrypted connection.
6. Portable devices should be safeguarded from theft or loss the same way as a personal credit card.
7. All portable devices will indicate method of return to IT Department if found. Any misplaced portable device must be immediately reported to the department administrating them.
8. All portable devices are subject to the same security guidelines as workstation units including restricting visibility of display in public areas.
9. All data contained on portable devices must be backed up on a regular basis according to the policies and procedures set forth by IT.
10. Portable media that leaves the County worksite must follow all portable device requirements.
11. Portable devices are to be synchronized only to a County-approved computer.
12. Disposal of any portable device must follow the guidelines in this policy.
13. Sensitive information stored on a laptop computer shall be in encrypted form using the processes defined by the IT Department and approved by the SO.

**27. Encryption**

### 27.1 Use of Encryption

Use of encryption on the County's information system will only be done using processes approved by the SO, and only for official County business. Users are forbidden to use encryption for any other purposes except for official County business.

### 27.2 Transmittal of Sensitive Information

Sensitive information that is to be transmitted on the County's WAN or via the Internet shall be encrypted. The requirement for encryption is set by the applicable department head. The IT Department sets and the SO approves the encryption processes to be used by the County to meet this requirement.

### 27.3 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.

### 27.4 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.

#### 27.4.1 Encryption Key Escrow

Copies of all encryption keys will be kept in escrow and accessible by the County Administrator and the IT Department.

## 28. Transfer of Computer Equipment and Media

### 28.1 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 approved by the SO that ensure that any previously stored information will not be recoverable.

### 28.2 Outside the County

As the County upgrades its computer systems, the County may decide to dispose of its old computers. Before any computer leaves County premises, IT shall be contacted and will ensure that all data stored on the computer is removed using methods approved by the SO ensuring that any previously stored information on the media is not recoverable.

## 29. Hardware and Software Configuration

Configurations and set-up parameters, as defined by the IT Department 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 SO. IT reserves the right to disconnect from the County network any hardware or software application with configuration or parameters that are not compliant.

## 30. 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 to prevent tampering and unauthorized use. Information technology equipment must be protected from power surges, power failures, water damage, overheating, fire, and other physical threats.

**31. 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 STG shall be followed.

**Appendix A: SECURITY OFFICIAL JOB DESCRIPTION**
**Title:** Security Official

**Reports to:** Senior Executive

**Overview: The security official is the individual responsible for Cortland 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 security official is expected to help management create an environment in Cortland 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 Cortland County's workforce and management in implementing sound security practices and preventing security incidents.

3. Serves on the County's HIPAA Security Task Group that prepares security policies and 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 Cortland County remains in compliance with HIPAA Security Rule requirements.

5. Promptly investigates security incidents brought to her/his 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 Cortland 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 Cortland 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 ePHI.

2. Familiarity with Cortland County's operations and information systems and other computer applications 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 Cortland 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 Security Task Group:**

1. Implement sound security practices to prevent security incidents.
2. Prepare security policies and 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 Security Official, 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 Security Official in promptly investigating security incidents brought to her/his attention and pursuing resolution in conjunction with the Security Official as needed.
5. Implement Cortland 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.

082008

**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 of security**: 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.

**Consumer reporting agency**: an agency that assembles or evaluates consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties. A list of such agencies is compiled by the state attorney general and will be furnished to the County upon request.

**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 Administrator 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.

**Firewall:** A Security device that creates a barrier between an internal network and an external network.

**Handheld Computer**: Small computer running portable 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:** Considered to be any adverse event that threatens the confidentiality, integrity or accessibility of information resources.

**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.

**Instant Messaging (IM):** The ability to exchange short messages online with co-workers or others. IM solutions can take several forms.

**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 the IT Department.)

**LAN**: Local Area Network

**Laptop Computer**: Portable 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.

**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.

**PDA:** Personal Digital Assistant. Handheld device used to store a variety of personal information such as contacts and schedule. Capable of storing digital data such as PHI.

**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.

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

**Portable Storage Device:** Device used for storing data such as USB flash drives.

**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 permit access 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 destruction of information.

**SO:** Security Official—appointed by the County Administrator; see job description.

**STG:** Security Task Group. At a minimum, this group is composed of the SO, a representative from IT and departments that are considered "covered entities" under HIPAA---Department of Social Services, Mental Health Department, and Health Department. See responsibilities listed within the Security Official Job Description, Appendix A.

**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.

**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 County entity, political subdivision, its employees, third party contractor(s) or business associate(s), or any other individual(s) authorized by such entities to access a system for legitimate government purpose.

**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.