County of
Clinton

Information Technology
Information Security Policy

Rules and Regulations for County Information Systems

Table of Contents

Purpose.........5
Scope.........6
Policy Organization.........6
County Information Assets.........6
Information System Criticality.........7
The County's Information System Criticality Levels
Determining the Criticality Levels
Annual Inventory Report of County Information Systems Criticality Levels
Information Technology Asset Inventory
County Information Security Administration.........8
Centralized Responsibility for Information Security
Information Technology Network and Technical Support Team Responsibilities
Network Administrator Responsibilities
Information Security Incident Response
Annual Information Systems Planning Process Required
Risk Analysis, Assessment and Management
Periodic Independent Review of Information System Controls
Accrediting Hardware and Software
Configuration Control
Current Information Security Manual Required
Amending the Information Security Policy
User Responsibilities.........10
Information Security Training and Awareness.........11
Required Security Training
Security and Confidentiality Policy Statement
Responsibility for Security Training
Information Security Awareness
Information Recovery
Theft of Information
Departmental Agreements
Third Party Agreements
Vendor/Contractor Agreements
Contingency Planning.........12
Contingency and Disaster Planning Document
Contingency Planning Responsibility
Periodic Testing
Acceptable and Unacceptable Use Policy.........13
Acceptable Use
Unacceptable Use
Privacy Expectations for Users.........14
County Information Security Audit Policy.........15
Security Tools.........15
Information Technology Staff Permission to Use Security Tools
Copyright and Licenses.........15
Disclosure of Information System Vulnerabilities.........16
Reporting suspected Security Incidents / Violations.........16
Violations.........16
Non-Compliance
Disciplinary Review
Absence of Guidelines

Breach Notification Policy..**16**
The County's Information Systems Connections...**16**
Internal
External Connections
Modems
Remote Access to the County's Network by County ITS Users
Third Party Access
Intermunicipality Agreements
System Privileges / Access...**17**
Granting System Privileges
Inactive Accounts
Need-to-Know
Group or Shared Accounts Prohibited
Guest and Anonymous User-Ids
Revoking System Access
User Status Change
County Staff Departure (Voluntary or Termination)
Two User-IDs Required for Privileged Information Technology Users
Vendor's Access Privileges
Screen Savers
Protecting Sensitive Information
Login-In / Log-Off Process..**18**
Network Log-In Banner Required
User Authentication Required
Login Prompts
Disclosure of Incorrect Log-In Information
Limited Number of Log-In Attempts
Password Policy...**19**
Initial Password set-up
Vendor-Supplied Default Passwords
Security Compromised
Accountability
Password Disclosure
Positive Identification to reset Password
Password Selection
Password aging
Tracking Previous Passwords Used
Password Storage
Changing Passwords
Information Systems Backup..**20**
Backup Responsibility
Backup Plan
Backup Testing
Offsite Storage of Backups
System Logs..**21**
System Logs Enabled
Accountability and Traceability for All Privileged System Commands
Reviewing Logs in a Timely Manner
Clock Synchronization
Malicious Code...**21**
Malicious Code Detection
Protecting Portable Computing Devices from Malicious Code
Initial Scanning of Software
Malicious Code Eradication

Laptop / Netbook / Tablet Security 21
Avoiding Loss of a Laptop
Protecting Information Stored on the Laptop
Laptop Backup
Laptop Information Encryption
Wireless Security 22
Encryption 22
Use of Encryption
Transmittal of Sensitive Information
Storage of Sensitive Information
Encryption Keys
Encryption Key Escrow
Online Banking Policy...22
Transfer of Computer Equipment and Media 23
Internal to the County
Outside the County
Hardware and Software Configuration...23
Firewalls and Intrusion Detection...23
Physical Security...23
Systems Development and Maintenance 24

Appendix A: Glossary...25

1. Purpose

Access to Clinton County's (hereinafter referred to as the County) information systems has been provided to all authorized County employees and approved interns, consultants, service providers and contractors performing business on behalf of a County agency/department (hereinafter referred to as County Information Technology Systems Users [County ITS Users]) for the benefit of providing service to the residents of Clinton County. All County ITS Users have a responsibility to maintain and protect the County's information assets against accidental or intentional disclosure or compromise. Each County ITS User also has the responsibility to maintain and protect the County's public image and to use the County's information systems in a productive manner.

Information is essential to all County services. As a result, information security is a critical requirement 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 or due to County ITS 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 County ITS Users are responsible and productive users of the County's information resources, the following policy document for using the County's information systems has been established. This policy is applicable to the County's internal computer network (County Wide Area Network) as well as interconnections with systems outside the County WAN (Internet).

- **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 that are adequate to achieve an acceptable level of risk for each system will be implemented through the guidance of this policy.

This policy establishes procedures and requirements designed to protect and maintain the availability, integrity, confidentiality and non-repudiation of information and information resources.

- **Availability:** Systems and data being operational, accessible, functional and usable upon demand by an authorized entity, e.g., a system or a user.
- **Integrity:** Data not being altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.
- **Confidentiality:** Information not being made available or disclosed to unauthorized individuals, entities or processes.
- **Non-Repudiation:** Unquestionable proof of the origin of, the content integrity of a transaction or of data and the receipt and optionally the acceptance of a transaction or of data, such that refutation of any of these is not possible.

Effective information security is a team effort involving all County ITS Users who access 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:

- Establish an evolutionary, risk managed information security program to defend against internal and external threats.
- Establish a management structure to address the County's information security operation.

- Require all County ITS Users to:
  - be knowledgeable of acceptable County information system usage,
  - understand their information security responsibilities,
  - be held accountable for their actions.

2. Scope

The policies contained in this document are applicable to all 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 owned or operated by the County. They also cover any computer and communications devices that are 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 departments, County employees and other authorized users having access to or using information systems and resources of the County. It is the responsibility of all County ITS Users to protect the County's information systems and information from accidental or intentional misuse or destruction.

3. Policy Organization

Clinton County's Information Security Policy consists of two parts: a policy for use, ownership, management, disclosure and processing information on the County's information systems and a technical policy which details technical aspects of the County's information security.

4. County Information Assets

Information, such as data, electronic mail, documents and software, are agency assets. In determining the value of an asset, consideration should be given not only to the sensitivity of the information, but also to the consequences of unauthorized disclosure, modification, destruction, or unavailability of the information. The value of these assets will determine the level of controls needed to provide adequate safeguards, backup and access controls. However, ownership, custodial responsibility and rights to these assets must first be established.

- **Departmental Records.** A "record" includes any information kept, held, filed, produced or reproduced by, with or for a department in any form or media including, but not limited to, reports, statements, examinations, memoranda, opinions, folders, files, books, manuals, pamphlets, forms, papers, designs, drawings, maps, images, photos, letters, microfilms, computer tapes or discs, rules, regulations or codes, websites, or E-mail.
- **Property of a Department.** All records, software, and hardware that are part of a department's information system are considered property of the department and should be used for departmental business purposes only. In furtherance of a governmental purpose, a department head or designee has the right to examine all information residing in or transmitted by means of departmental communications or computing devices.
- **Designation of Responsibility.** A department head or designee has the ultimate responsibility to ensure that all departmental information resources, regardless of medium, are used, maintained, disclosed and disposed of according to law, regulation or policy.
- **Copyright and Licensing of Vendor Hardware and Software.** Departments must adhere to copyright laws and licensing agreements.
- **Records Retention and Destruction.** Departmental information must be retained and/or destroyed in accordance with records retention schedules developed in cooperation with the State Archives and Records Administration (SARA) and policies and procedures established by the agency, unless required otherwise by applicable laws.
- **State and Federal Access, Privacy and Confidentiality Laws.** All information, regardless of the medium

in which it is maintained or communicated, is subject to pertinent State and federal laws governing access, the protection of privacy and prohibitions against unauthorized disclosure.

- **Access Categories - Classification of Information.** Information classification provides a means for separating information into categories with different protective requirements. Departments should determine, in advance, the extent to which information should be disclosed to specified users. Determinations should be made based on the nature of the information and the duties of departmental employees. The following general categories of information serve to provide guidance in identifying appropriate users or recipients:
- **Public Information** is information accessible under Freedom of Information Law and is available to any person, notwithstanding one's status or interest.
- **Restricted Information** pertains to information which is not public information, but can be disclosed to or used by departmental representatives to carry out their duties, so long as there is no legal bar to disclosure.
- **Confidential Information** is information which is protected by law. Access to confidential information is prohibited unless permitted by an exception in law.

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

Physical Access / Security
The department shall put into place appropriate safeguards to limit physical access to any computer or computer related device.

- **Secure Locations.** Mainframe, servers, switches, routers and other essential computer devices shall be stored in a location that protects them from unauthorized physical access. Physical access to such equipment potentially provides access to information stored therein.
- **Location Selection.** Physical locations for all computer related equipment should be selected to protect against equipment and information loss by flood, fire, and other disasters, natural or man-made.
- **Review of New Connections to Outside Sources.** Proposed access to or from a network external to the county must be reviewed and approved by the department head or designee before establishment of the connection.
- **Review of Installation.** Installation, upgrade, changes or repairs of computer equipment and computer related devices (hardware, software, firmware) must be reviewed by the county for potential physical security risks.
- **Platform-specific Physical Security.** Platform-specific physical security must be established, implemented and periodically reviewed and revised as necessary to address physical vulnerabilities of that platform.
- **Laptop, Notebook and Portable Computer Devices.** Portable computing devices must not be left unattended at any time unless the device has been secured. All portable computing devices will be encrypted for security purposes.

5. Information System Criticality

The County's Information System Criticality Levels
All County information systems shall be classified according to their criticality to County operations into one of three categories: Business Vital Systems, Business Essential Systems, or Public Systems.

Business Vital Systems
Business Vital Systems are systems that require a high degree of protection to ensure the confidentiality, integrity or availability of the information stored on them. These systems are absolutely vital to County business operations. This includes systems and data whose destruction, improper use or disclosure could have a substantial and perhaps disastrous impact on the County's business operations.

Business Essential Systems
Business Essential Systems and the information stored on them are essential to continued County business operations and need special protection. However, their destruction, improper use or disclosure

of the information stored within would not be disastrous to County business operations. These systems require less protection than vital systems, but more than public systems.

Public Systems

Public Systems contain only Public information that requires no special protective measures required for confidentiality. Availability and integrity of the information is still a concern. County operations could be accomplished without the system for a limited time.

Determining the Criticality Levels

The criticality level of County information systems is determined during the risk assessment process.

Annual Inventory Report of County Information Systems Criticality Levels

The Information Technology Applications Support Team, on an annual basis, is required to submit an inventory report (to include application software information) to the Information Security Officer (ISO), in a format set forth by the ISO, that will at a minimum list all County information systems and dedicated communications links, along with their associated criticality level.

Information Technology Asset Inventory

Information Technology Network and Technical Support Team is required to provide an annual inventory of information systems (using the Annual Inventory Report of Information Systems Criticality Level created by the Information Service Application Support Team) detailing all existing hardware, system software and communication link information. The format will be determined by the ISO.

6. County Information Security Administration

Centralized Responsibility for Information Security

The responsibility and authority for the County's information security is formalized in the Information Security Officer (ISO). The ISO is responsible for maintaining, coordinating and directing specific actions to maintain the confidentiality, integrity, availability and non-repudiation of County information resources as specified in the Clinton County Information Security Policy document. The ISO reports to the Director of Information Technology of Clinton County. The ISO is responsible for:

- Developing policies, standards, procedures and guidance for implementing the County's information security policy;
- Providing information security education and awareness training to County employees;
- Ensuring information security is integrated with the County's business use of information technology;
- Developing the use of specific methodologies and processes for information security (e.g., risk management);
- Reviewing and bringing forth to the County Director of IT amendments or modifications to the County's information security policy, which will then be brought forth to County Department Heads and if need be to the County Administrator and the County Legislature.
- Reviewing the County's information security posture;
- Heading the investigation in the event the County's information resources are compromised either from internal or external sources;
- Ensuring the County's information security policy is adhered to;
- Investigating data security violations and report findings to the County Director of IT.

Information Technology Network and Technical Support Team Responsibilities

The Information Technology Network and Technical Support Team, with guidance from the ISO, are 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 required.
- Harden systems (by removing unnecessary services and patching necessary ones) before connecting them to the network.
- 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 Information Technology Operations Team.
- 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. Documentation must be stored in a secure location.
- Establish and maintain effective and secure telecommunications capabilities for/with off-site facilities.
- Identify common user deficiencies and ensuring these are passed to the ISO for inclusion in the 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.

Network Administrator Responsibilities

Network 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 appropriate access control measures;
- Install patches expeditiously to identified system vulnerabilities;
- Educate the ISO and users on security issues;
- Activate the appropriate security capabilities of servers and desktop systems;
- Review logs in a timely manner.

Information Security Incident Response

Information Security Incident Response Team

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

Incident Response and Procedures Plan

The ISO working with the County's ISIRT shall develop an incident response plan and procedures to be used in the event of an incident.

Recovery Actions

The ISIRT will take appropriate measures to secure the County's information resources from further compromise. After a security incident, the ISIRT will follow the list of approved recovery actions to bring the affected system(s) on-line and into service.

Investigating the Security Incident

In responding and investigating the incident the ISIRT must keep in mind the following objectives:

- 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.
- Report the incident to the appropriate supervisor, unit manager or department head.

Comment [H1]: We added this bullet.

Annual Information Systems Planning Process Required
The Director of IT and the ISO must annually 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.

Risk Analysis, Assessment and Management
On behalf of the Director of IT, the ISO 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.

Periodic Independent Review of Information System Controls
An independent review by an outside party of information security controls must be conducted annually (provided funding is allocated by the County Legislature). These reviews must include efforts to determine both the adequacy of controls and compliance with them. Those in the County responsible for implementing and maintaining security controls or computer systems must not perform the reviews.

Accrediting Hardware and Software
The ISO is responsible for developing an accreditation process for 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.

Configuration Control
The Information Technology 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.

Current Information Security Manual Required
The ISO must prepare, maintain and distribute information security manual(s) describing the County's current information security polices and procedures. The manual(s) for employees must be appropriate to the employee's job function.

Amending the Information Security Policy
The Clinton County Information Security Policy shall be amended when there is a need to align the policy with current County business practices, change in laws or technological change. The ISO is responsible for drafting new policy statements or amendments to policy for review by the Director of IT. The County Administrator, Director of IT and appropriate committees shall approve amendments to policy. Once approved, the amended policy will be in effect.

7. User Responsibilities

County ITS Users are responsible for adhering to the policy and the security controls governing the resources under their control to prevent unauthorized disclosure of information, ensuring effective and accurate processing and maintaining continuity of operations for accomplishing the County's mission.

Each County ITS User is responsible for the context of all text, audio or images they place or send over email, voicemail, the Intranet or Internet. Fraudulent, harassing or obscene (inappropriate) messages are prohibited. No abusive, profane or offensive language shall be transmitted through the County's systems. County ITS Users who wish to express personal opinions on the Internet should obtain their own accounts and use systems other than the County's.

Information stored, processed and transmitted on the County's information systems are owned by the County, and as such is a County resource in the custody of the County ITS User. It is the County ITS User's responsibility to ensure all sensitive County information is adequately protected at all times -- in the manner prescribed by the information owner. When data is transferred from the County ITS User's custodial responsibility to another County ITS User, each County ITS User accepts the same responsibility of continued protection.

County ITS Users shall:

- Become aware of the sensitivity/criticality of the information they handle and apply appropriate protective measures when handling the information.
- Coordinate the connection of Personal Communications Devices (PDAs) with the ISO and Information Technology.
- Coordinate the connection of devices with RF capabilities (e.g., wireless access points, wireless LANs) with the ISO and the Information Technology Department.
- Use only legal software that is licensed to the County on County computers.
- Scan all files and software for malicious code prior to execution.
- Use robust network passwords and change them as required.
- Never share ID or passwords with another user.
- Never document passwords and put them on or near the computer (i.e. sticky notes under keyboards, on monitors, etc.)
- Lock the screen, log off, or activate screensavers with password protection to protect the County's information when they are left unattended.
- Never release non-public County information unless prior authorization from the information owner has been obtained.
- Not disclose sensitive County data to other County Staff other than on a need-to-know basis.
- Secure any physical copies of sensitive County data such as tapes, CD's and printouts when left unattended.
- Backup data on a regular basis if data is not kept on a server that IT backs up.
- Become familiar with indicators of virus infection and report operational anomalies to Information Technology Technical Support, ISO or the Director of IT.
- Report all discovered security vulnerabilities and/or computer security concerns to their supervisor, ISO, Director of IT or the County Administrator.
- When working at home, take reasonable measures consistent with workplace standards to safeguard access to County information resources (e.g., computers, networks, and data).

8. Information Security Training and Awareness

Required Security Training

All County ITS Users are to be provided with sufficient information security training and support reference materials appropriate to their job responsibilities. For County ITS Users, who are new County employees, the information security training will be incorporated into the Human Resources new employee orientation program. For County ITS Users, who are not County employees (e.g., consultants), the ISO 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.

Security and Confidentiality Policy Statement

All County ITS Users are required to sign a security and confidentiality policy statement, before they are given access to the County's information resources, that they have read, understood and had been given the opportunity to ask questions concerning the County's information security policy. The security and confidentiality policy statement shall include language as follows: County ITS Users shall be required to sign the security and confidentiality policy statement annually. Access to and use of County information resources shall be terminated for any County ITS User who does not sign a security and confidentiality policy statement.

Responsibility for Security Training
The ISO in conjunction with the Information Technology Department is responsible for providing the material and conducting the training sessions for new County ITS Users and the annual refresher security training to remind all County ITS Users of their responsibility and obligations with respect to information security.

Information Security Awareness
The ISO is responsible for developing and conducting an information security awareness program throughout the year.

Information Recovery
All systems must have backup and recovery procedures that are documented, maintained and stored off site. The department should make every effort to test these procedures on an annual basis.

Theft of Information
A department must take measures to prevent the theft of county information resources.

Departmental Agreements
Departments with systems that exchange data with/to any other entity must sign a formal agreement with that entity to adhere to specific agreed upon security protocols related to data exchange.

Third Party Agreements
All agreements with third parties such as vendors, other government agencies, or contractors must include requirements to adhere to Clinton County's Information Security policies.

Vendor/Contractor Agreements
All vendor agreements shall contain a requirement that any county information obtained as a result of such an agreement shall be the property of the County and shall not be utilized, including but not limited to secondary release or disclosure, without written authorization of the county.

9. Contingency Planning

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.

Contingency Planning Responsibility
The Director of IT is responsible for contingency planning. The ISO is responsible for providing technical guidance for all information security contingency plans.

Periodic Testing
The Information Technology Department shall periodically test the County's information technology contingency plan(s).

10. Acceptable and Unacceptable Use Policy

Acceptable Use
County ITS 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, commercial profit or to facilitate unethical or criminal activities. The County's computers and networks are only to be used for official County business. The only exception is access to the Internet for personal use during non-duty hours (before and after work, breaks and lunch time).

Communications by County ITS Users from a County e-mail address to newsgroups or listservs must contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the County's, unless the posting is in the course of County duties and reflects the official view or opinion of the County.

Unacceptable Use
The following activities are, in general, prohibited. County ITS Users may be exempted, in writing, from these restrictions during the course of their legitimate job responsibilities.

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

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

System and Network Activities
The following activities are strictly prohibited, with no exceptions.

- 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 not appropriately licensed for use by the County.
- 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.
- 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.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- 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.
- Using a County computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Making fraudulent offers of products, items or services originating from any County account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- 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 the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless performed by authorized Information Technology staff.
- 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., Information Security staff).
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the user's host (for example, denial of service

attack).
- 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.
- Providing information about or lists of County Staff to parties outside County government, unless the information is considered public.
- Using encryption on County information systems without written authorization by the Director of IT or the ISO.
- Intentionally changing hardware and software configurations as deployed by Information Technology without written authorization from the Director of IT or the ISO.

Email and Communications Activities
The following activities are strictly prohibited, with no exceptions.

- 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).
- Any form of harassment via email, telephone or paging whether through language, frequency or size of messages.
- 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.
- Unauthorized use or forging of email header information; a.k.a. e-mail spoofing.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within the County's networks of other Internet/Intranet service providers on behalf of, or to advertise, any service hosted by the County or connected via the County's network.
- Posting the same or similar non business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Web Servers, MUDs, Network Games, Listservs, Other Computer Applications on County Information Systems

County ITS 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, WinMX, Madster) or listservs running on County information systems without written consent from the Director of IT or the ISO.

Instant Messaging
County ITS Users are prohibited from using Instant Messaging (IM) on any County information resource, unless authorized in writing by the Director of IT or the ISO.

Security Circumvention
County ITS Users must not attempt to compromise information system security measures in any way. Incidents involving unapproved system hacking or cracking, password cracking, 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 ISO in consultation with the Director of IT, County ITS users, including Information Technology 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. County ITS Users, including Information Technology staff, found in violation may face disciplinary measures, which may include immediate dismissal.

11. Privacy Expectations for Users

County ITS Users should be aware that Internet/Intranet related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing and FTP's are the property of the County and thus County ITS 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.

The County respects the privacy of all network users and indiscriminate monitoring of user communications shall not occur. However, exceptions to this policy may be made under specific conditions such as a program causing disruption to the network or other shared resources, or the suspected violation of the County's guidelines of acceptable use and behavior or state and federal law.
Such monitoring will only be performed by authorized County personnel with compelling business or security reasons and only with the approval of the Director of IT or the ISO, and in consultation with legal and human resources. 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 activities and inspect 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 ISO 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 (labs, offices, cubicles, storage areas, etc.);
- Access to interactively monitor and log traffic on County networks.

13. Security Tools

The ISO in consultation with the Director of IT is authorized to acquire and employ the appropriate security tools necessary to ensure confidentiality, integrity and availability of the County's information system resources. These tools shall include mechanisms for recording, detecting and correcting security problems. They may also include password and network security checkers, intrusion detection systems, hardware/software firewall technologies and other information security tools (a.k.a. hacking tools -- some security tools are dual use -- security and hacking). Possession or use of security tools by other than specifically authorized Information Technology staff is prohibited.

Information Technology Staff Permission to Use Security Tools
Information Technology 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 Director of IT or the ISO before such tools are acquired and used on the County's information resources.

14. Copyrights and Licenses

Failure of County ITS Users to observe copyright or license agreements may result in disciplinary action or legal action by the copyright owner and by the County. County ITS 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 license violations, and did not take any action to correct and to prevent copyright and licensing violations. Violations by County ITS Users will be referred to Human Resources and Legal for further 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 Information Security Incident Response Team (ISIRT) will place all hardcopy or electronic documents, notes, memos on investigative results, in a secured file to which only the ISIRT members have access.

16. Reporting Suspected Security Incidents / Violations

It is the County ITS User's responsibility to immediately report, in confidence; all suspected policy violations, system intrusions, virus infections and other conditions that might jeopardize the County's information security to their supervisor, the County Administrator, the County Director of IT or the ISO.

17. Violations

Non-Compliance
All County ITS 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.

Disciplinary Review
The County shall have in place a review process based on current employee disciplinary processes to address information security policy violations.

Absence of Guidelines
The absence of specific guidance covering a particular situation does not relieve County ITS Users from exercising the highest ethical standard applicable to the circumstances. When in doubt, contact your immediate supervisor or the ISO.

18. Breach Notification Policy

New York State Technology Law Section 208 requires local governments to establish an information breach notification policy. The Records Access Officer will notify county residents whose private information was, or is reasonably believed to have been, acquired by a person without a valid authorization. The disclosure will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

19. The County's Information Systems Connections

Internal
The County's information infrastructure shall have separately defined, organization-based logical domains (where practical), each protected with suitable security perimeters and access control mechanisms.

External Connections
The Director of IT or the ISO must approve all external connections before any external connection is made and all connections must adhere to standards and procedures for security as set forth by Information Technology. 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 County Director of IT and the ISO. Non-compliance in maintaining such a list or not providing the list to the Director of IT and the ISO allows Information Technology to terminate any connection to the County Network so as to preserve a secure environment. The Director of IT and the ISO are granted the authority to direct staff to

remove connection points on the County's network under the Director of IT's control that pose a security risk to the County network.

Modems
The use of modems on the Clinton 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 Director of IT and the ISO. Only the Director of IT and the ISO have the authority to approve the use of a modem connection. The allowed modem connection shall be in accordance to the security standards and procedures set forth by the Information Technology for such connections.

Remote Access to the County's Network by County ITS Users
Remote access to the County WAN by County ITS Users shall only be via methods that ensure the security of the County's network and are approved by the ISO and the Director of IT. Only the Director of IT or the ISO have the authority to grant County ITS Users remote access to the County's network, and only after reviewing with the Department Head the need for such access and access requirements. Any user requesting this access will be required to submit a Request Form signed by their Department Head and the Director of Information Technology.

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 Director of IT and the ISO are the final approval authority for such agreements

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, standards and procedures for connecting to the County WAN. The Director of IT and the ISO are the final approval authority of such agreements.

20. System Privileges / Access

Granting System Privileges
Requests for new user-IDs and changed privileges must be in writing and approved by the Department Head and information owner and submitted to Information Technology before the system administrator fulfills the request.

Inactive Accounts
Accounts that have been inactive for a period of 90 days will be deactivated. These "deactivated" accounts will be permanently removed on a regular basis.

Need-to-Know
The information system privileges of all County ITS users, based upon the information security policy, are to be restricted based on the "need-to-know." This means privileges on County information systems must not be extended unless a legitimate business need for such privileges exists.

Group or Shared Accounts Prohibited
Information systems access control and audit ability shall be achieved via the use of user accounts 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 Director of IT and the ISO can grant a waiver to this requirement if adequate justification is provided and security measures are determined to be appropriate.

Guest and Anonymous User-Ids
Anonymous and "guest" user-IDs are prohibited and must be disabled from all County information systems.

Revoking System Access

User Status Change

Department Heads must promptly report all significant changes in County ITS User duties as it relates to information access to the information owners. System administrators must promptly revoke privileges no longer needed by County ITS User. The County shall have a process in place by which changes in a County ITS User's duties as they relate to information and network access are communicated to Information Technology.

County Staff Separation (Voluntary or Termination)

In the event a County ITS User separates, the County is required to have in place a process that ensures that the employee's access to County information resources is disabled. As part of the process a separation checklist is to be used whenever an employee leaves County service. Information Technology shall promptly disable the County ITS User's access to the county's information systems and information (e.g., disabling employee's account(s)).

In the case of termination, the Department Head is required to immediately notify Information Technology by phone of the need to disable the employee's access to all County information resources and accounts. This is followed up by the separation checklist from Human Resources.

Two User-IDs Required for Privileged Information Technology 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.

Vendor's Access Privileges

Vendor must not have access privileges by default to the County's information systems. All such accounts on vendor supplied equipment or applications must be disabled. Vendors needing to provide maintenance on equipment via remote access must coordinated with the Director of IT or the ISO. All vendor activity will be closely monitored and logged by Information Technology.

Screen Savers

County ITS Users are required to have password protected screen savers activated. After a certain period of no activity, based on the sensitivity of the information, the screensaver blanks the screen. The County ITS User will need to re-authenticate to resume work.

Protecting Sensitive Information

If the information accessed by County ITS User on a computer is classified as HIPAA related, County ITS 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

Network Login Banner Required

Every County system, where technically feasible, must employ a login 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) understand he/she is subject to monitoring.

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.

Login Prompts

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

Disclosure of Incorrect Login Information
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.

Limited Number of Login Attempts
Access to an account will be locked out if a reasonable number of unsuccessful login attempts occur during a preset time period. The number of allowable failed login attempts is dependent on the criticality of the system and the sensitivity of the information. The length of the lockout is dependent on the criticality of the system and the sensitivity of the information contained in the system.

22. Password Policy

Initial Password Set-up
Wherever system software permits, the initial passwords issued to a new County ITS 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 a County ITS User forgets a password. The initial password must be difficult to guess, which means it should not follow any predictable patterns, such as any words or numbers representing the user’s personal or organizational information.

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.

Security Compromised
Whenever the security of an information system has been compromised, or if there is a convincing reason to believe an 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.

Accountability
County ITS 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.

Password Disclosure
County ITS Users must never disclose their password(s) to anyone or to any entity under any circumstances. If access to certain County resources is required for business purposes, the Information Owner should approve the access. Under no circumstances should any County ITS User provide access to said resources via sharing a password or through other means. If a password is unintentionally disclosed, the County ITS User shall immediately change the password.

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 reset a password, or issue a new password.

Password Selection

All county employees are required to adhere to a strong password policy. The specifications are as follows:

- They must be at least eight characters in length
- They may not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- They must contain characters from **three** of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)
- Complexity requirements are enforced when passwords are changed or created

Password Aging
All County ITS Users will be automatically required to change their passwords periodically -- at least once every ninety (90) days, or less depending on the sensitivity of the information and the criticality of the system.

Tracking Previous Passwords Used
If system software permits, a history file of passwords must be employed to prevent users from reusing passwords.

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 system or in other locations where unauthorized County ITS 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 County ITS Users might discover them.

Changing Passwords
County ITS Users are required to change their password immediately if they suspect that their password has been disclosed.

23. Information Systems Backup

Backup Responsibility
To protect the County's information resources from loss or damage, Information Technology is responsible for the installation of automated backup hardware and/or software on all servers. All critical information must be backed up on a regular basis. Information shall be backed up according to its criticality level as defined by its owner. 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.

Backup Plan
The Director of IT in consultation with the ISO shall formulate a backup plan for all County information resources.

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.

Offsite Storage of Backups
The backup itself must be carefully protected. A copy of the backup will be made and stored offsite as determined by the nature of the information and set forth by the information owner. Offsite is synonymous with "out of the building." The offsite storage location must provide evidence of adequate fire and theft protection and environmental controls.

24. System Logs

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 guess passwords, attempts to use privileges that have not been authorized, modifications to production application software, modifications to system software, changes to user privileges and changes to logging subsystems.

Accountability and Traceability for All Privileged System Commands
All special privilege commands issued on the County's information systems must be traceable to individuals via comprehensive logs.

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. Automated means are required to aid in this tedious process.

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

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.

Protecting Portable Computing Devices from Malicious Code
Information Technology shall develop a process for County ITS 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). County ITS Users have the responsibility to ensure that their portable computing device has the latest protection against malicious code by following the policy, standards and procedures set forth by Information Technology.

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

Malicious Code Eradication
County ITS 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 Information Technology staff.

26. Laptop / Netbook / Tablet Security

Avoiding Loss of a Laptop
County ITS Users must take proper care to prevent their laptop from being stolen.

Protecting Information Stored on the Laptop
Laptop Backup
It is mandatory for all County ITS Users using laptops to back-up important files on a regular basis according to the standards and procedures set forth by Information Technology.

Laptop Information Encryption
Sensitive information stored on a laptop computer shall be in encrypted form using the processes defined by the ISO.

27. Wireless Security

Clinton County Information Technology reserves approval for all deployment or introduction of wireless infrastructure devices to the county’s network. Any violation of this policy will result in an immediate disconnect from county resources and a possible confiscation of the unapproved equipment. Disclosure of wireless credentials is strictly prohibited without

28. Encryption

Use of Encryption
Use of encryption on the County's information systems will only be done using processes approved by the Director of Information Technology, and the ISO, and only for official County business. County ITS users are forbidden to use encryption for any other purposes except for official County business.

Transmittal of Sensitive Information
Sensitive information that is to be transmitted on the County’s WAN or via the Internet shall be encrypted.

Storage of Sensitive Information
Sensitive information stored on County information systems must be encrypted. In addition any archived (back-up copies) sensitive information also need to be encrypted.

Encryption Keys
Encryption keys used by the County shall be treated as confidential information. Access to encryption keys shall be strictly limited on a need-to-know basis.

Encryption Key Escrow
Copies of all encryption keys will be kept in escrow and accessible by the Director of IT and the ISO.

29. Online Banking Policy

Each county department that performs these activities must define the following:

- What online banking and EFT activities will be used
- Who is authorized to initiate electronic transactions
- Who will approve electronic transactions
- Who will transmit electronic transactions
- Who will record electronic transactions
- Who will review and reconcile electronic transactions

These definitions should be reviewed and updated regularly.

Segregation of Duties
At least two individuals should be involved in each electronic transaction. The authorization and transmitting functions should be segregated and, if possible, the recording function should also be delegated to someone who does not have either approval or transmitting duties.
Generally, the same controls should be used for electronic disbursements through online banking as apply to the manual preparation of checks.

Payments made using electronic funds transfer services cannot circumvent laws, regulations, and/or internal control policies.
It is critical that bank accounts be monitored on a timely basis, at least every two days, for unauthorized or suspicious activity.
Any suspicious activity should be immediately reported to banking officials and/or law enforcement.
Authorized Access Controls

- Maintain unique Login Accounts for each Employee for each electronic banking site.
- Login information should be saved in a secure place (i.e.: not taped to monitor or under keyboard)
- Electronic banking sites are only allowed to be accessed from WIRED county network based computers. (No wireless devices)
    - This ensures:
        - Malicious website filtering
        - Email threat protection
        - Client Based Virus/Malware protection

30. Transfer of Computer Equipment and Media

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, proper measures need to be employed to ensure all data is removed from the computer's storage media before the computer is relocated to another location within the County. Information Technology, using methods approved by the ISO to ensure any previously stored information will not be recoverable, shall conduct the removal of such data.

Outside the County
As the County upgrades its computer systems, there is a need to dispose of old equipment. Before any computer leaves County premises, Information Technology shall be contacted and will ensure all data stored on the computer is destroyed or disposed of in accordance with all applicable federal and state laws, rules and regulations. Acceptable methods include Wiping, Degaussing or Physical Destruction. IT will maintain a log of all storage media that has been disposed of and/or destroyed. The log will include the date, type of device, manufacturer, serial number (if one exists) and the method of sanitation or destruction used.

31. Hardware and Software Configuration

Configurations and set-up parameters, as defined by the ISO and the Director of IT, for deployed hardware and software must comply with County security policies and standards. 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 ISO and the Director of IT. Information Technology reserves the right to disconnect from the County network any hardware or software application whose configuration or parameters are not compliant.

32. Firewalls and Intrusion Detection

Clinton County Information Technology has implemented a firewall configuration to decrease the vulnerability of computerized information access by unauthorized individuals. The firewall has the capability of analyzing network traffic and allowing or blocking specific instances, providing the critical protection for County resources. The firewall also provides important logging and auditing information, which will be periodically reviewed, for compliance with the county's security objectives and to detect any possible unauthorized intrusion.

33. Physical Security

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

34. 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. Whenever new systems are procured or developed or existing systems are significantly modified by either in-house or vendor personnel, the standards and procedures developed by the Director of IT and the ISO shall be followed.

Appendix A: Glossary

Account ID: Same as User Name.

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.

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: Countermeasures or safeguards that are the technology that are needed to satisfy the requirements set forth by 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.

County ITS User: County Information Technology Systems User. See definition of User.

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

Data: Data shall be defined as any information created, stored (in temporary or permanent form), files, produced or reproduced, regardless of the form of media. Data 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.

Encryption: The cryptographic transformation of data to render it unintelligible through an algorithmic process.

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

IM: See definition of Instant Messaging.

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 Owner: An individual or organizational unit having responsibility for making classification and control decisions regarding the use of information.

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 Security Architecture: A framework designed to ensure information security principles are defined and integrated into business and IT processes in a consistent manner.

Instant Messaging: The ability to exchange short messages online with co-workers or others. IM solutions can take several forms. They can use an existing Internet based service, or they can be an Intranet only solution implemented and controlled within an IT department. The latter is significantly more secure than the former, but lacks access to outside business partners.

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 facilitate data transmission and exchange, which all use the standard Internet protocol, TCP/IP, to communicate and share data with each other.

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 upon actual or suspected unauthorized access and events for investigation and resolution.

ISO: Information Security Officer.

IT: Information Technology.

Malicious Code: Is programming or files that are developed for the purpose of doing harm; examples of which are viruses, worms, and Trojan horses.

Non-repudiation: The availability of irrefutable proof of the provenance of, the content integrity of a transaction or of data, and the receipt and, optionally the acceptance of, a transaction or of data, such that refutation of any of these is not possible.

Principles: General comprehensive, fundamental and durable statements or guidelines which underpin an architecture – relate to the role, use or direction of security in an organization.

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

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

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.

Security Policy: The set of criteria for the provision of security services based on enterprise-wide rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

Sensitivity: The measurable, harmful impact resulting from disclosure, modification, or destruction of information.

Standard: Sets of rules for implementing policy. Standards make specific mention of technologies, methodologies, implementation procedures and other detail factors.

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.

Technical Security Review: A technical security review would consist of reviewing the controls built into a system or application to ensure they still perform as designed. It would also include reviewing security patches to ensure they have been installed and are operational, review of security rules such as access control lists for currency, testing of firewall rules, etc.

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 (a.k.a. County ITS User): shall be defined as any authorized County employee, approved interns, consultants, business associates, service providers and contractors performing business on behalf of a County agency/department for the benefit of providing service to the residents of Clinton County.

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

Virus: A program, usually malicious, 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 or violate system integrity. Vulnerability can be assesses in terms of the means by which the attack would be successful.

Worm: A worm is a self-replicating piece of software, usually malicious, similar to a virus, but requires to user action to activate it. A worm exploits weaknesses in operating systems and other applications to propagate itself to other systems.