Clinton County Information Security Policy

May 9, 2005

Table of Contents

1. Purpose

Access to Clinton County's (hereinafter referred to as the County) information systems has been provided to all authorized County employees, consultants, contractors, interns, volunteers, and temporary workers (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- **Expiration Date**: This policy remains in effect until superseded, amended, or canceled.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:

1. Establish an evolutionary, risk managed information security program to defend against internal and external threats.
2. Establish a management structure to address the County's information security operation.
3. Require all County ITS Users to:
   a) be knowledgeable of acceptable County information system usage,
   b) understand their information security responsibilities,
   c) 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: Managerial Policy and Technical Policy. Managerial Policy establishes policy for use, ownership, management, disclosure and processing information on the County's information systems. Technical Policy establishes policy for the detailed technical aspects of the County's information security.

Managerial Policy

4. County Employee Responsibilities

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.

Three responsibility classifications (**owner**, **custodian**, and **user**) are defined to assist County ITS Users in understanding their roles and responsibilities when using the County's information systems. County ITS Users may fall into more than one category.

- **Owner:** All information residing on the County's information systems must have a designated owner. Information owners determine the appropriate information sensitivity classification to be applied to the information. Owners are responsible for deciding which County ITS Users will be permitted to access the information, and the uses to which the information will be put. ***All information owners are required to submit an annual report to the Information Security officer (ISO), in a format set forth by the ISO, listing the information of which they are owners.***

Discussion: *This would greatly strengthen the concept of "system ownership" being in the departments rather than Information Technology. This would also require the ISO to keep a list of all Information Systems within the County. This is a great step forward in recognizing where we have Information Systems and who is responsible.*

- **Custodian:** Information on the County's information systems must have a designated custodian. The custodian is responsible for protecting the information in accordance with the information owner's access control, data sensitivity and data criticality instructions.

    - At a minimum, the **custodian** is responsible for:
        - ensuring physical security for equipment, information storage, backup, and recovery is adequate;
        - ensuring a secure processing environment that can adequately protect the integrity, confidentiality, and availability of information is maintained;
        - developing and maintaining a business continuity 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 authorized access to an information asset by the owner. The user is responsible for 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.

Specific information security responsibilities shall be incorporated into all County ITS Users' job descriptions.

Discussion*: This policy statement will help County ITS Users understand their responsibilities and roles as it relates to the County's information. It is important that information have an owner, it is the owner of the information who is responsible for determining how sensitive and critical is the information to the County's functioning, and how the information will be used and by whom. Based on the information owner's input, the information custodian is able to take the necessary actions to secure the information with safeguards appropriate to the information's sensitivity and criticality. They will inform users on the proper use of information in their job duties. When in doubt, a user knows that they can contact the information owner to determine proper use of the information. Furthermore, the custodian, who is responsible for the information's security, knows how to protect the information. We will have to work with HR on adding Information Security responsibilities to job descriptions.*

5. Information System Criticality

5.1 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**.

5.1.1 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.

5.1.2 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.

5.1.3 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.

5.2 Determining the Criticality Levels

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

5.3 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.

Discussion*: The intent of this policy is to specify standard terminology used to classify systems within the County. The classifications reflect how important the application, system, or information is to the County. The criticality rankings will assist the Information Security Officer (ISO) and the Information Technology Network Team in designing network infrastructure and developing contingency and security plans. These categories should serve as a determinant factor when creating security procedures and controls, auditing procedures, system backup procedures and standards and intrusion detection. For example, the business vital systems should be placed in a centralized office protected with the highest security policy; systems backup should be conducted on a routine basis; redundant intrusion detection tools should be installed; and audit logs should be reviewed daily. The policy also requires that an up-to-date listing be maintained of County systems and their criticality levels.*

5.4 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.

Discussion: *All information technology assets must be identified before security protections can be placed upon them. This policy requires the County to prepare an annual information systems inventory detailing all existing hardware, software, and communication links. This allows the County to properly secure these assets and plan for contingencies. A current inventory is also useful to management for planning purposes.*

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 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:

a. Developing policies, standards, procedures and guidance for implementing the County's information security policy;
b. Providing information security education and awareness training to County employees;
c. Ensuring information security is integrated with the County's business use of information technology;
d. Developing the use of specific methodologies and processes for information security (e.g., risk management);
e. 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.
f. Reviewing the County's information security posture;
g. Heading the investigation in the event the County's information resources are compromised either from internal or external sources;
h. Ensuring the County's information security policy is adhered to;
i. Investigating data security violations and report findings to the County Director of IT.

Discussion: *The intent of this policy is to denote a focal point, the Information Security Officer (ISO) for information security at the County, and defines his or her responsibilities. Also, the policy defines the reporting relationship of the ISO to the Director of IT.*

6.2 Information Technology Network and Technical Support Team Responsibilities

The Information Technology Network and Technical Support Team, with guidance from the ISO, 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 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.

6.3 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.

6.4 Information Security Incident Response

6.4.1 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.

6.4.2 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.

6.4.3 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.

6.4.4 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.

Discussion: *The intent of these policy statements is for there to be an Information Security Incident Response Team (ISIRT) responsible for handling information security incidents within the County. Such a team will have developed a set of contingency plans on how to handle an incident and the subsequent investigation. The ISIRT is responsible for the forensic analysis to clean the system in the event of a security incident. Procedures must be in place to document the investigation so that evidence is not destroyed or modified in the course of the investigation that will make prosecution that much more difficult. The investigation must provide sufficient information so that Information Technology can take steps to ensure that: (1) a similar incident cannot reasonably take place on the County's information systems; (2) security measures have been reestablished and strengthened. The findings of the ISIRT should be documented in detail for future references.*

6.5 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.

6.6 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.

Discussion: *A properly performed risk analysis and management assessment will result in a prioritized list of information most at risk and which could cause unacceptable losses to the County. The prioritized list provides direction as to where information security measures should be applied and how much to spend. The assessment provides management information on which to make fact-based decisions on the amount of risk management is willing to bear. The risk assessment needs to occur before any application, system or service is deployed.*

6.7 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.

Discussion: *The intent of the policy statement is to have a periodic independent security review of the County's information systems by an outside party. An outsider's independent review can bring a fresh perspective into an organization's security review. Also, it helps maintain the vigilance of the computer and network staff.*

6.8 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.

Discussion: *The intent of this policy statement is to ensure that no new hardware or software is placed on the County's information systems unless the ISO has evaluated it from a security perspective. This is important so that the security in place is not compromised by some new application. If security concerns are noted, then the staff will take the appropriate controls to mitigate them.*

6.9 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.

Discussion: *Having a documented process of how changes are to occur allows for stricter configuration control. In other words, new software, patches, hardware will not be installed in a haphazard manner. The documentation will allow the Information Technology Staff and the ISO to know what is running on what. In the event a new*

vulnerability is found, security personnel will be able to quickly ascertain whether the County's systems are vulnerable.

6.10 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.

Discussion: *The intent of this policy statement is to put into policy that a current information security manual(s) must be maintained and available to the County's employees. The manual(s), updated in a timely manner, describes how things related to security will be done at the County. It should be a detailed guidance for County ITS Users and Information Technology Staff. Without specific guidance, County ITS Users will be at a loss concerning what is permitted and what is not permitted. The manual(s) need to be relevant to the employee's job responsibilities. The information security needs of a secretary are quite different than that of a network administrator; the manuals should reflect that; otherwise, the manual may be too intimidating. Furthermore, different employees have a different need to know level. An example of such a security manual is the Clinton County Information Technology Policies and Procedures document for use by County Personal Computer and Terminal Workstation Customers (users). What will need to be done by Information Technology, is reconciling the policy wording in the Technology Policies document, with the wording in this policy document. It is envisioned that additional policies will be added to the Technology Policies document, based on what is in this policy. What can be done is to take the overall policy and extract all those policies that directly affect the user and produce a user version of the policy, much like what has been done with the Technology Policies document.*

6.11 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 security of the information 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 the email, voicemail, 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 as proscribed 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.
- Not connect a modem to a phone line while the same computer is connected to the County LAN without approval of the ISO.
- 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 password 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, floppy disks 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, data).

8. Information Security Training and Awareness

8.1 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.

Discussion: *The intent of this policy will be to ensure every County ITS User is made aware of the importance of information security as it relates overall to the County and to their job responsibilities. Training needs to be reflective of the employee's job duties (e.g., a system administrator will receive different training than an administrator, or a supervisor at the County). By signing a statement acknowledging the training, the County ITS User acknowledges they have read and understood the training.*

8.2 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.

Discussion: *The intent of this policy is to ensure every user is aware of their responsibilities as a user of the County's information resources. This provides a document that the user acknowledges the policy. In this way the organization has a legal way of taking action including firing the person based on policy violations, according to terms that the person agreed to by signing.*

8.3 Responsibility for Security Training

The ISO in conjunction with the Information Technology Department are 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.

8.4 Information Security Awareness

The ISO 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.

Discussion: *Policy intent is to state that a document must be in place for contingency planning that specifies what steps need to be performed in the event of a contingency. The plan and the procedures need to be detailed in advance. In an emergency, time can be crucial.*

9.2 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.

9.3 Periodic Testing

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

Discussion: *Need to make sure that information technology contingency plans are workable. Staff needs the practice of going through such drill. Such drills point out deficiencies in information technology contingency plans. Lessons learned can improve the information technology contingency plans.*

10. Acceptable and Unacceptable Use Policy

10.1 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.

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.

10.2 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.

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 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 fraudulent offers of products, items or services originating from any County account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. 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.

10. Port scanning or security scanning is expressly prohibited unless performed by authorized Information Technology staff.
11. 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).
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).
14. 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.
15. Providing information about or lists of County Staff to parties outside County government, unless the information is considered public.
16. Using encryption on County information systems without written authorization by the Director of IT or the ISO.
17. Intentionally changing hardware and software configurations as deployed by Information Technology without written authorization from the Director of IT or the ISO.

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).
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 email 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", "Ponzi" or other "pyramid" schemes of any type.
7. Use of unsolicited email originating from within the County's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the County or connected via the County's network.
8. 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

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 ISO.

10.2.4 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.

10.2.5 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 dismissal, in accordance with New York State Civil Service Rules and Regulations and bargaining unit agreements.

Discussion: *Topics above are self-explanatory. The policy aim is to control the behavior of County ITS users.*

11. Privacy Expectations for Users

County ITS 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 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.

Discussion*:* *The purpose of this policy puts all county ITS Users on notice that all information on the County's information systems belongs to the County and is considered public. County employees and authorized users have no expectation of privacy using the County's information systems. The County has the right to monitor and review all information on the County's information systems without consent of any County user.*

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.

Discussion: *This policy statement will provide the authority for ISO to conduct a security audit on any County system and will have the requisite access.*

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. 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.

Discussion: *The policy statement aims to limit who in the County has the right to acquire and use security tools (a.k.a. hacking tools). No one but authorized County Staff ought to be using security tools. Since many system compromises are accomplished by those internal to the organization, security tool possession by unauthorized County Staff needs to be prohibited.*

13.1 Information Technology Staff Permission to Use Security Tools

Information Technology staff, who in their job duties will require the use information security tools (a.k.a. hacking tools) must obtain permission from their immediate supervisor and from the County Director of IT or ISO before such tools are acquired and used on the County's information resources.

Discussion: *The permission form for the use of security (a.k.a. hacking tools) serves two main purposes: 1) maintain accountability of what security tools are in use in the County and by whom; 2) protects authorized personnel using these security tools from penalties if in the event, and they will happen, these tools break things on the network or the authorized user is able to see information traversing across the network that they normally would not have access to. Therefore, it is important for the authorized user's supervisor as well as the ISO and the Director of IT to sign-off on the use of these tools. The supervisor and the ISO and Director of IT need to understand the risk associated with the use of such a tool and the possible consequences. By giving written permission (by signing a permission form) the supervisor as well as the ISO and the Director of IT acknowledge and accept the risk.*

14. Copyright 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.

Discussion: *This policy statement aims to mitigate the risk to the County if a County ITS User installs unlicensed software. The County can show that it has a policy prohibiting unlicensed software to be installed, and the associated enforcement mechanisms. The policy puts County ITS Users and supervisory personnel on notice that they will be liable for violations, and that the matter will be referred to Human Resources and Legal.*

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.

Discussion: *Information on County security is always to be treated as Confidential Information with a need-to-know.*

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.

Discussion: *The intent of this policy is to make County employees aware of their responsibility to report security incidents and violations, and to whom suspected violations are to be reported.*

17. Violations

17.1 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.

17.2 Disciplinary Review

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

17.3 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.

Discussion: *The intent of the above policy statements is to stress the importance of information security, and that significant disciplinary action may result if a County ITS User is found to be in violation. However, every violation will be reviewed by a committee according to a set of procedures developed by the committee. The review process will attempt to ascertain the severity of the violation, whether it was accidental or intentional, and whether the offender's behavior is chronic. The County recognizes that not every instance can be covered in a security policy, and therefore expects County ITS Users to exhibit the highest ethical standards in all circumstances. County ITS Users are put on notice that they must report suspected security violations.*

Technical Policy

18. The County's Information Systems Connections

18.1 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.

Discussion: *The intent of the policy statement is to ensure that that all internal traffic must pass through a suitable security perimeter (e.g., firewall) to protect against internal malicious activity and against penetration by outside sources.*

18.2 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.

Discussion: *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.*

18.3 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.

Discussion: *This policy eliminates security vulnerabilities created by dial-up connections using modems. Modems are considered a weak link in security. A user using a modem on a PC, which is on a LAN on the Clinton WAN, to connect to another network bypasses the County's perimeter security, thus allowing an external network direct connection to the County's network. For example, a user may install a modem on his or her computer so they can access the Internet through their personal Internet Service Provider (ISP), 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.

18.4 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.

Discussion: *This policy aims at setting the means by which remote access to the County's network will be granted to County ITS Users. Such access will be provided via methods that ensure the security of the County, for example, such access can be granted using Virtual Private Networks (VPNs). It is the responsibility of the Department Head to make the case for remote access for their employees.*

18.5 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

Discussion: *The intent here is to make sure that there exits an agreement between the County and any third party wanting to connect to the County's network. The agreement will outline the third party's responsibilities and will hold them liable if they are not compliant with the agreement.*

18.6 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.

Discussion: *The intent here is to make sure that there exits an agreement between the County and any municipality wanting to connect to the County's network. The agreement will outline the municipality's responsibilities.*

19. System Privileges/Access

19.1 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.

Discussion: *The intent of this policy statement is to have a process by which to grant User ID's and grant privileges.*

19.2 Inactive Accounts

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

Discussion: *The intent of this policy statement is to ensure inactive accounts are cleaned up.*

19.3 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.

Discussion: *The intent of this policy statement is to limit access to the County's information on a need to know basis. County ITS Users ought not to have privileges beyond those necessary to perform their job function.*

19.4 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 ISO can grant a waiver to this requirement if adequate justification is provided and security measures are determined to be appropriate.

Discussion: *The intent of this policy statement is to maintain the audit ability of individual user actions. All actions performed on the County's information systems must be associated with only one individual, and not to a group of individuals. In the event of a security incident, the user who performed the fault action can be easily traced, which enhances the overall security level of the County's network.*

19.5 Guest and Anonymous User-Ids

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

Discussion: *The use of such IDs will compromise the security level of the County's internal network. There is no traceability to who used the account. In many instances, outside attackers look for such default accounts.*

19.6 Revoking System Access

19.6.1 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.

Discussion: *The intent of this policy is to ensure that there exists a process by which the County ITS User's access to County information systems is reflective of the County ITS User's job responsibilities.*

19.6.2 County Staff Separation (Voluntary or Termination)

In the event 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.

Discussion: *The intent of this policy is to ensure that a County ITS User who leaves voluntarily or is terminated does not have continued access to the County's information resources. All of the County ITS User's accounts need to be disabled.*

19.7 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.

Discussion: *The intent of this policy is to differentiate a privileged user's usage of the County's information systems between their responsibility of administering or securing the system, and their use as a normal user (e.g., checking email, surfing the web, composing documents). This policy makes log analysis and review easier because a great deal of irrelevant information is not included in the detailed logs of privileged user activities.*

19.8 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.

Discussion: *In many instances there exist accounts in information technology that enable vendors to remotely access and service equipment or applications. The passwords associated with these accounts need to be under the control of the County's Information Technology Department. Access to IT equipment or applications via these accounts must only be done in conjunction with Information Technology, otherwise changes made by a vendor when servicing the device or application may adversely affect the County's security. In addition, this policy forces Information Technology to disable these accounts whose existence and default passwords are well known.*

19.9 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.

Discussion: *Screen savers ensure that unauthorized persons are not able to use microcomputers or view the data stored on them while authorized users are away from their desks. Re-authentication may be as simple as providing the correct password to the screen saver, or may involve two-factor authentication*

19.9.1 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.

Discussion: *Prevents unauthorized users from gaining access to confidential information when the authorized user is away. After all, an unauthorized user has free reign to an authorized user's access when a computer is left unattended and logged into the system. The user in this case is required to either enable a password protected screen saver, or is required to log-off (if a screen saver is not technically feasible) before they step away from the workstation.*

20. Login / Logoff Process

20.1 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.

Discussion: *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. This is equivalent to a non-trespassing sign. In addition, users are put on notice that their actions may be monitored, and consent to the monitoring.*

20.2 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.

Discussion: *Use of a user-ID in conjunction with a password is the minimum for authentication to County information systems. Other authentication forms (e.g., token-based, smart-card, biometric) need to be considered for remote user authentication, or to systems containing sensitive information.*

20.3 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.

Discussion: *The intent is to provide the least amount of information possible to a potential intruder. An intruder may be using automated means to find networks of interest. If the login prompt gives the intruder the information that the system belongs to such and such organization, the name of the organization may spark interest in the hacker. Information about the operating system and other technical information provided will only give additional information to the intruder making it easier for him or her to attack and possibly compromise the system.*

20.4 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 userID or to an invalid password. Instead, the person logging in must simply be informed that the login process was incorrect.

Discussion: *The intent of this policy statement is to make sure that no revealing information is given to someone who fails to login. For example, if the system informed the person logging in that their userID is valid, but the password is invalid, then the would be intruder would know that he or she has a valid userID. It is simply prudent to*

say that the login was not successful; instead of stating which part of the login process was improper.

20.5 Limited Number of Login Attempts

Access to an account will be locked out if an unreasonable number of unsuccessful login attempts occurs 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.

Discussion: *Reasonable limits need be set as to the number of allowable login attempts. The number of failed login attempts allowed before the account is disabled is dependent on the criticality of the system. Whether the lockout is reset automatically after a preset length of time or requires system administrator intervention depends on the criticality of the system and the sensitivity of the information contained in the system.*

21. Password Policy

21.1 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.

Discussion: *The intent of this policy statement is to ensure that County ITS Users will be forced to change their initial passwords when they are given accounts, otherwise the user may continue to use the password. It is important that the initial password not be based on some predictive pattern because if there is a time delay from the time the account is set up and the user actually logs-in for the first time, the account can potentially be compromised by other employees or an outside attacker who knows the pattern of initial passwords (e.g., employees first name).*

21.2 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.

Discussion: *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.*

21.3 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.

Discussion: *If a system intrusion occurs, there is the possibility a packet sniffer used by the intruder may have captured passwords. Therefore, it is prudent to change passwords, so the intruder cannot gain access to the system via a password that has been cracked.*

21.4 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.

Discussion: *This maintains the audit ability of user actions, so the user cannot say "it wasn't me who did such and such because I let so and so use my account."*

21.5 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.

Discussion: *County ITS Users are made aware that they should never under any circumstances divulge their password to anyone. This policy is set forth as a means of counteracting social engineering attacks, where an attacker calls an unsuspecting user and tries to manipulate them into divulging their password. Many times the attacker assumes the role of a superior as a means to intimidate the user into providing their password.*

21.6 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 reset a password, or issue a new password.

Discussion: *The intent of this policy statement is to prevent social engineering, whereby an intruder calls the system administrator claiming to be so and so (usually someone of authority in the organization) and demanding that the password be immediately changed.*

21.7 Password Selection

The first line of defense against an attack against the County's information systems is the use of robust passwords. County ITS Users are to refer to the document titled "Clinton County Password Guidelines" for guidance on how to choose a robust and difficult-to-guess password.

Discussion: *Using passwords conforming to the guidelines set out in "Clinton County Password Guidelines" is essential to lower the possibilities for them to be easily guessed or cracked by unauthorized users using software readily available to the hacker community.*

21.8 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.

Discussion: *The intent of this policy is to limit the potential affects in case a password is compromised without the password owner becoming aware. The setting of the time period is critical, if it is too short users will be frustrated of having to constantly change their passwords, and will be tempted to write-down the password. Note, the policy states at least every ninety days, which suggests that if conditions warrant it (type of information protected) the period may be lessened to reflect the sensitivity or the criticality of the information or system.*

21.9 Tracking Previous Passwords Used

If system software permits, a history file of passwords must be employed to prevent users from reusing passwords

Discussion: *The intent of this requirement is to minimize the possibility for the password to be compromised. Potential intruders may try a previously known password.*

21.10 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 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.

Discussion: *The intent of this requirement is to minimize the possibility for the password to be compromised due to unintended disclosure of the password to unauthorized users.*

21.11 Changing Passwords

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

Discussion: *The intent of this requirement is to minimize the possible damage from a compromised password.*

22. Information Systems Backup

22.1 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.

22.2 Backup Plan

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

Discussion: *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 due to other reasons such as power failure, natural disasters, system breakdown, hardware problems or any other unforeseen incident, backup files may be used for recovery purposes. The backup plan needs to address full and incremental backups.*

22.3 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.

Discussion: *Backup hardware and software sometimes fail. Without testing to make sure that the backup hardware and software is working correctly, the County may be lulled into a false sense of security that its information is being backed-up. Very important to validate that back-ups are actually happening, and that the information can be retrieved from the back-up media.*

22.4 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.

Discussion: *In the event of a contingency (e.g., building burning down or a flood) it is prudent to keep back-up media at a different location. Better to have back-ups in multiple locations. Offsite storage is one of those issues that go hand-in-hand with Contingency Planning. A determination needs to be made on how far the off-site storage needs to be from the County office building and from the contingency plan site where County Information Technology will be housed in the event of an emergency. For example, if the County office building was hit with a biological or chemical agent.*

23. System Logs

23.1 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 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.

Discussion: *Sets in policy the requirement that system logging, especially security events, be logged. The County can require that all future applications have security logging capability.*

23.2 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.

Discussion: *The intent of this policy statement is to make sure that the use of privileged commands used by system administrators, security folks, and by intruders is dutifully logged.*

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

Discussion: *Sets in policy that logs need to be reviewed. The frequency of the review is dependent on the sensitivity of the information and the criticality of the system. Each information owner and custodian will need to determine the appropriate period for reviews. Automated means will need to be employed to shift through the volumes of information in the logs; this will require purchasing software to accomplish this.*

23.4 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.

Discussion: *Having the correct time across all systems will aid in the auditing of County systems, and in the forensic investigation of a security breach. We do not have this capability yet but need to implement it at least for servers.*

24. Malicious Code

24.1 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.

Discussion: *Malicious code, such as computer viruses, computer worms, and "Trojan Horses", are unauthorized programs that can self-replicate, attach to other programs and spread through various information storage media and/or across a network. Symptoms of malicious code can include much slower computer response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of systems. This policy sets forth the requirement of using malicious code detection software (a.k.a. anti-virus software), and that the software be automatically updated. Such software is only as good as its last update.*

24.2 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.

Discussion: *Keeping anti-virus signatures at current levels on portable computing devices (e.g., laptops) poses a challenge. These devices need to connect to a network on a regular basis, so that the latest anti-virus signatures can be pushed to the portable computing device. The policy also sets forth that County ITS Users of laptop computers are ultimately responsible for making sure their laptop is protected with the latest protection.*

24.3 Initial Scanning of Software

Software on all County systems must be scanned for malicious code and copied or backed up prior to its initial 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.

Discussion: *Need to make sure that software to be installed does not have any malicious code in it. There have been occurrences that packaged software has had malicious code in it, because the manufacturer's network (where the software was recorded onto media) was compromised. In addition, Information Technology may want to consider having on its intranet a page of often requested and downloaded utilities. This serves an important security purpose, in that if a County ITS User needs a utility, they can go and download a copy from the County intranet, knowing the copy is safe to use on the County WAN, in other words the software doesn't hide a virus or a Trojan, because Information Technology would have verified that the software is free of malicious code. There exist many instances where hackers have attached malicious software to popular downloadable utilities in the hope that a user will download an infected utility*

24.4 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.

Discussion: *This ensures that any malicious code is properly eradicated.*

25. Laptop Security

25.1 Avoiding Loss of a Laptop

County ITS Users must take proper care to prevent their laptop from being stolen.

Discussion: *Puts county employees on notice that they should use common sense in preventing their lap top computer from being stolen.*

25.2 Protecting Information Stored on the Laptop

25.2.1 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.

Discussion*: Even if laptop is lost or stolen, the information on the laptop has been backed-up.*

25.2.2 Laptop Information Encryption

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

Discussion: *Laptop computers are attractive to common thieves and those involved in industrial espionage. In many instances, the laptop computer is not what is of value to the perpetrator, but the information stored on the computer. So in order to prevent the compromise of the information stored on the laptop, sensitive information shall always be*

encrypted using the processes defined by the ISO. For example, one would not want an encryption technique that stores the key in a weakly protected password file that is on the laptop itself.

26. Encryption

26.1 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.

Discussion: *The intent of this policy statement is to prevent the misuse of encryption technology and/or the haphazard use of such technology. Encryption use can lead to a false sense of security; the encryption may not be secure enough. Or, encrypted information cannot be recovered because the key is lost, or a disgruntled employee can hold the information for ransom. By requiring all employees to follow the encryption processes as defined by the Director of IT and the ISO enough precautions and safeguards would have been put in place to prevent the possibility of using an insecure method, or facing the situation where important information cannot be recovered. As part of the encryption process, it is envisioned that the Director of IT and the ISO will develop some sort of key escrow account, whereby authorized County personnel can always access encrypted information. The policy also states that encryption can only be used for official business, and that no personal use of encryption is allowed on County information systems or by County ITS Users. Information Technology staff needs to be able to decrypt any message, if need be, sent or received by a County ITS User.*

26.2 Transmittal of Sensitive Information

Sensitive information that is to be transmitted on the County's WAN or via the Internet shall be encrypted.

Discussion: *The information owner sets the requirement for encryption. The Director of IT and the ISO will need to set the encryption processes to be used by the County to meet the requirement.*

26.3 Storage of Sensitive Information

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

Discussion: *Encrypting stored sensitive information adds another security layer to the defense in depth concept. Encrypting archived information prevents someone with access to the back-up tapes to access sensitive information.*

26.4 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.

Discussion: *The encryption keys need to be tightly controlled; otherwise the encrypted information's confidentiality or even its integrity can be compromised*

26.4.1 Encryption Key Escrow

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

Discussion: *This is to prevent the possibility that encrypted information is not recoverable because a key has been lost, or an employee is holding the County hostage.*

27. Transfer of Computer Equipment and Media

27.1 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, 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.

27.2 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, Information Technology shall be contacted, and Information Technology will ensure all data stored on the computer is removed using methods approved by the ISO; ensuring any previously stored information on the media is not recoverable.

Discussion: *As the County upgrades its computers and moves computers in its organization, donates or sells them to other institutions, the County needs to ensure that the information entrusted to the County is not inadvertently made public. Deleting a file does not actually delete the file on the system's media (e.g., hard disk, floppy). When a file is deleted, only a flag in the directory is set denoting that the file has been deleted. The physical representation of that file remains on the magnetic media until those blocks have been written over by another file. The electronic media needs to be sanitized using proven utilities that assure that data previously stored on the media is not recoverable. Otherwise data entrusted to the County may be compromised. In some instances, depending on the sensitivity of the information stored on the drive, the drive may need to be physically shredded. This all depends on the classification of the information and the security requirements set forth by the information owner.*

28. 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.

Discussion: *This policy aims at prohibiting County ITS Users or County Entities from changing configurations and set-up parameters of hardware and software. Network and system administrators are also put on notice, that they are not to change any configuration unless it has been approved in advance. Network and systems administrators can fallback on this policy when undue pressure comes from customers (e.g., County departments) asking for changes. Any change made from the configuration can potentially compromise overall network security.*

29. 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 usage. Information technology equipment must be protected from power surges, power failures, water damage, overheating, fire and other physical threats.

Discussion: *Physical security is a prerequisite to information security, thus non-authorized physical access to PBXs, hubs, routers, firewalls, servers, and other networking equipment needs to be prevented by physically securing the equipment in locked rooms. Even with the most sophisticated software access controls, the County's information systems can readily be compromised if the room in which the networking equipment is located is unlocked, or the wrong people have access to it. The space in which the equipment is located must protect it against fire, flooding, and other types of disasters both natural and man-made.*

30. 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.

Discussion: *This policy aims at ensuring that whenever any new system is to be developed or procured, or significantly modified a process must be followed. Studies show that that organizations adding controls after a business application goes into*

production will pay 10 times more than those organizations who built-in security during the development process. The process as developed to address how Clinton County ought to develop or procure systems, and the maintenance of systems – making sure that security is considered throughout the system development/procurement life cycle.

Revision History

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 county entity(ies), political subdivision(s), their employees or third party contractor(s) or business associates, or any other individual(s) who are authorized by such entities to access a system for legitimate government purpose.

User Name: The name which a computer system user is assigned that uniquely identifies them on the County's network, or on a specific information system on the County's network. It is the name with which a user logs in to the network, or the specific information system on the network.

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 uses exploits weaknesses in operating systems and other applications to propagate itself to other systems.