County of Clinton

137 Margaret Street
Plattsburgh, New York 12901

Information Technology Policies & Procedures

Rules and regulations for use of the
County of Clinton's
Management Information System

Table of Contents

Chapter

1

Use of the Internet

Introduction

Technology should be used to help government serve people. The Internet is a significant tool in that respect-- it is a worldwide telecommunications "network of networks" that can allow citizens and business to access information, and receive goods and services in ways that are better, cheaper and faster. It provides for resources such as electronic mail, Usenet, file transfer, remote login, gophers, and web sites. The fastest growing technology are World Wide Web servers or "Web Sites," which have the capability for text, graphical, and audio presentation of government information.

County Departments should use the Internet to help carry out their program missions. The Internet can facilitate communication and disseminate knowledge; encourage collaborative projects, resource sharing, and service provision; foster innovation and build a broader infrastructure to support the performance of professional, work-related activities.

Purpose/Strategic Direction

The purpose of this policy is to encourage County departments to establish Internet home pages and to make creative use of the Internet to facilitate customer service. The policy also addresses the responsibilities that come in doing so. While much of what follows may appear self evident, this policy is provided to cover:

- The overall coordination of Internet activities; and
- Department-level responsibilities for Internet activities.

Clinton County's presence on the Internet must be professional, comprehensive and coordinated. While the Data Processing Department will provide general coordination, the ultimate stewardship of Clinton County's presence on the Internet rests with individual departments. It is each department's responsibility to contribute to a professional, appropriate and coordinated presence for Clinton County on the Internet. Toward this end, each department's home page will be linked to the county home page. Also, home pages need to be formatted to present information clearly, in a way most useful to customers, and information should be linked logically and simply.

The Internet should be used to facilitate cost-effective and efficient business. This means that the Internet should be seen as a tool, a catalyst for streamlining department business practices, completing transactions without paper, reducing the number of forms and incoming calls, answering commonly asked questions, etc. In accordance with acceptable practice, departments should seek to link with other Internet sites such as State and Federal agencies to best serve their customers. County departments should *not* provide links to private businesses, unless all such businesses are provided equal access; unless

a formal business partnership has been approved; and/or unless the reason for the link is primarily educational in nature.

Core issues, when designing a web site include: the needs of customers in determining what information to provide and how to present it to ensure ease of use; security and confidentiality; and the professionalism and utility of the information provided.

Security

Since the Internet and its tools adhere to open and documented standards and specifications, it is inherently an unsecured network that has no built-in security controls. Confidential and sensitive information must not reside on Internet servers or systems, or be included in electronic communication available for public access unless proper, formalized security precautions have been established to protect privacy. It is the responsibility of each department to protect confidential and sensitive information where intentional, inappropriate or accidental disclosure of the information might expose the County or an individual to loss or harm. Departments must guard against even the perception that information given willingly by an individual to his or her government is in any way used inappropriately or without respect for the citizen's privacy. Internet resources are governed by existing privacy protection and confidentiality statutes, the same way other County's information is governed. Departments must take all appropriate measures to secure information systems and comply with county-wide security standards.

Acceptable Use Policy

It is the responsibility of each department to promulgate and insure compliance with Clinton County’s internet policy governing the acceptable and unacceptable uses of the Internet. This policy document includes statements regarding: legal issues such as copyrights; respect of privacy for others; harassment and threats; official use; prohibition of use for personal gain; prohibition of unauthorized access to other systems; results of violations of the policy, etc.

Department Responsibilities

Departments, within the parameters set herein, are encouraged to be creative in the development and use of the Internet. There are many examples of other counties on the Internet that have challenged conventional thinking and fully leveraged the advantages of this technology. In utilizing this technology, departmental responsibilities include assurances that:

- The information published on the Internet represents official agency information. Departments need to have management processes and internal policies in place that assure appropriate reviews and approvals;
- The department is in compliance with county-wide and agency-specific guidelines for security, and recommendations pertaining to formats and linkages;
- Information made available on county servers are timely, accurate, and appropriate and meets the county standards for quality;
- All Internet options, page links, graphic links, and URL links are verified regularly;
- Customers are provided timely and responsive acknowledgments and responses to queries and requests; and

- All personnel who have access to the Internet, electronic mail, and online services are aware of their responsibilities.

To ensure an overall consistency with the County's presence on the Internet, departments are asked to present their proposed home pages to the Data Processing department before they will be placed online. The DP department's role will be to coordinate a county-wide functional reference structure for organizing information across departmental lines in a manner that meets customer needs.

Archiving/Record Keeping

Business applications made accessible via the Internet must include procedures to capture and maintain secure, reliable records as evidence of transactions, such as may be needed to meet administrative, fiscal, legal, and other management accountability needs. Records must remain continuously accessible until disposal is authorized pursuant to a records disposal plan or schedule issued by SARA, the State Archives and Records Administration, in accordance with the State records management and archives law.

Clinton County Government's

Policy on Acceptable Internet Use

Introduction

The county connection to the global Internet exists to facilitate the official work of Clinton County Government. The Internet facilities and services will contribute broadly to the missions of the county.
The Internet connection and services are provided for employees and persons legitimately affiliated with the county for the efficient exchange of information and the completion of assigned responsibilities consistent with the county's statutory purposes.
The use of the Internet facilities by any employee or other person authorized by the county must be consistent with this Acceptable Use Policy and security policies.

Principles of Acceptable Use

Clinton County Internet users are required:

- To respect the privacy of other users; for example, users shall not intentionally seek information on, obtain copies of, or modify files or data, belonging to other users, unless explicit permission to do so has been obtained.
- To respect the legal protection provided to programs and data by copyright and license.
- To protect data from unauthorized use or disclosure as required by state and federal laws and agency regulations.
- To respect the integrity of computing systems: for example, users shall not use or develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system.
- To safeguard their accounts and passwords. Any user changes of password must follow published guidelines for good passwords. Accounts and passwords are normally assigned to single users and are not to be shared with any other person without authorization. Users are expected to report any observations of attempted security violations.

Unacceptable Use

Some examples of activity not acceptable for use of Clinton County Internet facilities include:

- For activities unrelated to the department's mission;
- For activities unrelated to official assignments and/or job responsibilities;
- For any illegal purpose;
- To transmit threatening, obscene or harassing materials or correspondence;
- For unauthorized distribution of county data and information;
- To interfere with or disrupt network users, services or equipment;
- For private purposes such as marketing or business transactions;
- For solicitation for religious and political causes;
- For unauthorized not-for-profit business activities;
- For private advertising of products or services; and
- For any activity meant to foster personal gain.

Department Rights
Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq), notice is hereby given that there are NO facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and user access requests, and will monitor messages as necessary to assure efficient performance and appropriate use. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

Limitation of Liability

The county reserves the right to log network use and monitor file server space utilization by users and assumes no responsibility or liability for files deleted due to violation of file server space allotments.
The county reserves the right to remove a user account from the network.
The county will not be responsible for any damages. This includes the loss of data resulting from delays, non-deliveries, or service interruptions caused by negligence, errors or omissions. Use of any information obtained is at the user's risk. Any computer connected to a network should have anti-virus software installed. The county makes no warranties, either expressed or implied, with regard to software obtained from this system. The county reserves the right to change its policies and rules at any time. The county makes no warranties (expressed or implied) with respect to Internet service, and it specifically assumes no responsibilities for:

- The content of any advice or information received by a user outside Clinton county or any costs or charges incurred as a result of seeking or accepting such advice;
- Any costs, liabilities or damages caused by the way the user chooses to use his/her department Internet access;
- Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the department. The department's Internet services are provided on an as is, as available basis.

Enforcement and Violations This policy is intended to be illustrative of the range of acceptable and unacceptable uses of the Internet facilities and is not necessarily exhaustive. Questions about specific uses related to security issues not enumerated in this policy statement and reports of specific unacceptable uses should be directed to Clinton County Data Processing. Other questions about appropriate use should be directed to your supervisor.

The county will review alleged violations of the Internet Acceptable Use Policy on a case-by-case basis. Clear violations of the policy which are not promptly remedied will result in termination of Internet services for the person(s) at fault, and referral for disciplinary actions as appropriate.

Chapter
2

Use of Electronic Mail

Introduction

Electronic mail (E-mail/Voice-mail) refers to the electronic transfer of information typically in the form of electronic messages, memoranda, and attached documents from a sending party to one or more receiving parties via an intermediate telecommunications system. E-mail/Voice-mail is helping County departments improve the way they conduct business by providing a quick and cost-effective means to create, transmit, and respond to messages and documents electronically. Well-designed and properly managed E-mail/Voice-mail systems expedite business communications, reduce paperwork, and automate routine office tasks thereby increasing productivity and reducing costs. These opportunities are, however, at risk if E-mail/Voice-mail systems are not managed effectively.

Purpose and General Policy

The purpose of this policy is to promote the use of E-mail/Voice-mail as an efficient communication and data gathering tool, and to ensure that County departments have the information necessary to use E-mail/Voice-mail to their best advantage in supporting county business. By establishing and maintaining compliance with a policy for appropriate use of E-mail/Voice-mail, risks and costs to departments can be mitigated while the valuable potential of this communication tool is realized.

County departments should ensure that E-mail/Voice-mail is used for internal and external communications that serve legitimate government functions and purposes. The information communicated over agency E-mail/Voice-mail systems is subject to the same laws, regulations, policies, and other requirements as information communicated in other written forms and formats. Each County department is responsible for promulgating policies, establishing management practices, and designing E-mail/Voice-mail applications that:

- support agency business;
- reduce legal and other potential risks;
- define managerial authority over E-mail/Voice-mail communications;
- describe the appropriate use of E-mail/Voice-mail communications;
- train employees in E-mail/Voice-mail use and policies; and
- provide for necessary records retention, accessibility, and protection.

Agencies with special requirements for information confidentiality (for example, confidential client records) may be required to establish additional safeguards to protect this data.

Departmental Responsibilities

Each department is responsible for promulgating and insuring compliance with the county's policy governing the use of E-mail/Voice-mail. Policies originally designed for paper correspondence or telephone use may not adequately apply to E-mail/Voice-mail. This policy document includes the following elements:

Proper Use:

- Defining proper business use and limiting personal use of E-mail/Voice-mail.
- Prohibiting the use of E-mail/Voice-mail for illegal and unethical activities or to misrepresent, slander or, otherwise jeopardize the legitimate interests of the County.

Departmental Responsibility:

- Establishing departmental control or ownership of E-mail/Voice-mail communications.
- Informing employees that E-mail/Voice-mail is not for personal use and should not be considered private or personal.
- Outlining the department's general approach to the provision of E-mail/Voice-mail services, as well as to the retention, maintenance and protection of E-mail/Voice-mail communications to ensure that records needed to support agency business operations are identified and remain accessible, usable, and reliable as long as they are needed. (Records have a specific meaning under Law -- see SARA's **Managing Records in E-mail/Voice-mail Systems** for more information.)
- Clarifying roles and responsibilities of managers, technical staff, and users for retaining, maintaining, and protecting E-mail/Voice-mail communications.
- The policy on acceptable Internet use fully applies to e-mail as well.

Legal Considerations:

- Providing that E-mail/Voice-mail messages related to agency business are government records under the Arts and Cultural Affairs Law and are subject to the same laws and requirements as other agency records, including general records management and program specific requirements.
- Providing that the Freedom of Information Law, Personal Privacy Protection Law, and discovery proceedings in legal actions apply to E-mail/Voice-mail communications.

A copy of Clinton County's E-mail/Voice-mail use policy is attached.

Assistance and Support

Clinton County has adopted the E-mail/Voice-mail policy guidelines proposed by the State Archives and Records Administration (SARA). SARA provides training and direct assistance on developing such policies and other records management issues raised by the use of advanced information technologies. It has published ***Managing Records in E-mail/Voice-mail Systems*** which provides agencies with guidelines for developing policies and establishing procedures for the effective management of records created and captured in E-mail/Voice-mail systems.

Clinton County Government's
Policy on E-mail/Voice-mail Use

Purpose and Goals
E-mail/Voice-mail is one of Clinton County's core internal and external communication methods. The purpose of this policy is to ensure that E-mail/Voice-mail systems used by county staff support county business functions to their fullest capacity. This policy advises staff and management of their responsibilities and provides guidance in managing information communicated by E-mail/Voice-mail.

Access to E-mail/Voice-mail Services
E-mail/Voice-mail services are provided to all staff as resources allow. To request access, contact Clinton County Data Processing.

Use of E-mail/Voice-mail
E-mail/Voice-mail services, like other means of communication, are to be used to support county business. Staff may use E-mail/Voice-mail to communicate informally with others in the county so long as the communication meets professional standards of conduct. Staff may use E-mail/Voice-mail to communicate outside of the county when such communications are related to legitimate business activities and are within their job assignments or responsibilities. Staff **will not use** E-mail/Voice-mail for illegal, disruptive, unethical or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interests of the County. Staff may not use e-mail for personal purposes.

Privacy and Access
E-mail/Voice-mail messages are **not** personal and private. However, program managers and technical staff may access an employee's E-mail/Voice-mail:

- for a legitimate business purpose (e.g., the need to access information when an employee is absent for an extended period of time);
- to diagnose and resolve technical problems involving system hardware, software, or communications; and/or
- to investigate possible misuse of E-mail/Voice-mail when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.

E-mail/Voice-mail messages sent or received in conjunction with county business may:

- be releasable to the public under the Freedom of Information Law;
- require special measures to comply with the Personal Privacy Protection Law.

All E-mail/Voice-mail messages **including personal communications** may be subject to discovery proceedings in legal actions.

Security
E-mail/Voice-mail security is a joint responsibility of county technical staff and E-mail/Voice-mail users. Users must take all reasonable precautions, including safeguarding and changing passwords, to prevent the use of the account by unauthorized individuals.

Management and Retention of E-mail/Voice-mail Communications
Applicable to all E-mail/Voice-mail messages and attachments

Since E-mail/Voice-mail is a communications system, messages should not be retained for extended periods of time. Users should remove all E-mail/Voice-mail communications in a timely fashion. If a user needs to retain information in an E-mail/Voice-mail message for an extended period, he or she should transfer it from the E-mail/Voice-mail system to an appropriate electronic or other filing system.

E-mail/Voice-mail administrators are authorized to remove any information retained in an E-mail/Voice-mail system that is more than 30 days old.
Applicable to records communicated via E-mail/Voice-mail

E-mail/Voice-mail created in the normal course of official business and retained as evidence of official policies, actions, decisions or transactions are records subject to records management requirements under the Arts and Cultural Affairs Law and specific program requirements.
Examples of messages sent by E-mail/Voice-mail that typically *are records* include:

- policies and directives,
- correspondence or memoranda related to official business,
- work schedules and assignments,
- agendas and minutes of meetings,
- drafts of documents that are circulated for comment or approval,
- any document that initiates, authorizes, or completes a business transaction,
- final reports or recommendations.

Some examples of messages that *typically do not constitute records* are:

- personal messages and announcements,
- copies or extracts of documents distributed for convenience or reference,
- phone message slips,
- announcements of social events.

Record Retention

Records communicated using E-mail/Voice-mail need to be identified, managed, protected, and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed, and accessible in existing filing system **outside the E-mail/Voice-mail system** in accordance with the appropriate program unit's standard practices.

Records communicated via E-mail/Voice-mail will be disposed of within the record keeping system in which they have been filed in accordance with a Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA). Program managers should consult with the County Records Management Officer concerning RDAs applicable to their program's records.
Users should:

- dispose of copies of records in E-mail/Voice-mail after they have been filed in a record keeping system;
- delete records of transitory or little value that are not normally retained in record keeping systems as evidence of agency activity.

Roles and Responsibilities

County executive management will insure that policies are implemented by department heads and supervisors. **Department heads and supervisors** will develop and/or publicize record keeping practices in their area of responsibility including the routing, format, and filing of records communicated via E-mail/Voice-mail . They will train staff in appropriate use and be responsible for ensuring the security of physical devices, passwords, and proper usage.

County network administrators and internal control (and/or internal audit) staff are responsible for E-mail/Voice-mail security, backup, and disaster recovery.

All E-mail/Voice-mail users should:

- Be courteous and follow accepted standards of etiquette.
- Protect others' privacy and confidentiality.
- Consider organizational access before sending, filing, or destroying E-mail/Voice-mail messages.
- Protect their passwords.
- Remove personal messages, transient records, and reference copies in a timely manner.
- Comply with county and departmental policies, procedures, and standards.

Policy Review and Update
The Data Processing department or designee will periodically review and update this policy as new technologies and organizational changes are planned and implemented. Questions concerning this policy should be directed to Data Processing staff.

Limitation of Liability

The county reserves the right to log network use and monitor file server space utilization by users and assumes no responsibility or liability for files deleted due to violation of file server space allotments.
The county reserves the right to remove a user account from the network.
The county will not be responsible for any damages. This includes the loss of data resulting from delays, non-deliveries, or service interruptions caused by negligence, errors or omissions. Use of any information obtained is at the user's risk. Any computer connected to a network should have anti-virus software installed. The county makes no warranties, either expressed or implied, with regard to software obtained from this system.
The county reserves the right to change its policies and rules at any time. The county makes no warranties (expressed or implied) with respect to Internet service, and it specifically assumes no responsibilities for:

- The content of any advice or information received by a user outside Clinton county or any costs or charges incurred as a result of seeking or accepting such advice;
- Any costs, liabilities or damages caused by the way the user chooses to use his/her department Internet access;
- Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the department. The department's Internet services are provided on an as is, as available basis.

Chapter

3

Information Security Policy

Introduction

Statement of Purpose

This document is designed to provide county departments with recommended *minimum* security policies for protection of assets inclusive of information, computers, and networks. These are high-level statements, independent of technology, designed to provide broad direction and goals. A companion document of standards and best practices is currently being drafted to supplement these policy statements and to provide guidance for implementing these recommended security policies. In advancing this policy, it is understood that individual business needs and requirements of individual departments may justify changing certain components of this policy. Changes should only be made after careful consideration and consultation with the procedures and best practices companion guide. This policy should be applied to all existing and future technology infrastructures.

Information Custodianship

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

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

laws governing access, the protection of privacy and prohibitions against unauthorized disclosure.

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

Physical Access Security

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

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

Information Security

The department is responsible for the security of all departmental information resources regardless of medium. Department specific procedures developed to conform with the following policies must be reviewed frequently to reflect changes in personnel and technology.

Information Security Administration Functions. Each department must formally delegate responsibility for all information security matters. Multiple individuals across organizational lines may be involved as long as there is a clear separation of duties and responsibilities which provide effective checks, balances and accountability.

For example, the individual responsible for systems security should not be a system administrator whose primary responsibilities are for maintaining and upgrading operating systems. Separating systems administration from security duties improves the security climate.

Lines of Communication. Lines of communication and responsibility for departmental security must be established, maintained and clearly defined. Alternative paths must be available in the absence of one of those individuals designated in the communications chain. These lines of communication must work in both directions either for the reporting upward of information security problems or the downward

communication of problem awareness such as information security alerts, potential virus threats and the like.

Logon Security. Access to computer systems requires identification and authentication. Any exceptions to this rule require appropriate departmental approval.

Remote Access to Departmental Information. Remote external access to the county network which contains restricted or confidential information requires extended authentication procedures. Any method for providing this remote access (e.g., modem, firewall) requires county approval before its installation.

External Network Access to County Information. External network access to the county network which contains restricted or confidential information requires at least a firewall. Firewalls provide network security similar to the installation of a perimeter security system on a building by blocking or permitting traffic.

Transaction Controls and Database Security. Transactions entered into the county's production databases must be checked for accuracy and authenticity.

Database management systems (DBMS) shall implement security and authorization subsystems adequate to protect against unauthorized access and modification.

Downloading Software. Each department must determine whether it will allow downloading of software from an external site. Departments that allow staff to download software must establish and follow procedures that ensure such software is adequately examined for undesirable effects before it is installed on county machines. (Note: Departments should be cognizant of incidental, unsolicited, or automatic downloading of executables by accessing an external site.)

Non-County Owned IT Components. Each department must develop procedures for defining use of non-county owned computer hardware and/or software for county business. In the case of software, vendor copyright and licensing agreements must be strictly adhered to. At the end of such use, all county information must be removed.

County Owned IT Components. County hardware should be reviewed and cleansed (sanitized) before being reassigned or discarded. Departments should maintain adequate documentation of hardware/software taken off site by employees.

Electronic Communications. When transmitting confidential information on an external network, departments shall employ a technology rendering the information unusable to an unauthorized or intercepting third party.

Virus Protection. All county computers should be equipped with up to date virus protection software.

County Security Management

Accountability and appropriate separation of duties and responsibilities are essential elements of security administration. In addition, departments must develop security awareness among all staff which include descriptions of practices intended to circumvent county security management.

- **Security Training.** All employees, agents and others who access county computer systems must be provided with sufficient training and supporting reference materials to allow them to properly protect county information.
- **Employment Changes.** Managers must report changes in employment status or job duties of their staff to the information security administrator. Personnel reports regarding employee status changes must be regularly provided to the designated information security administrator.
- **Audit Trails.** The department must maintain audit trail records sufficient to meet the requirements of the law, the needs of the county's internal controls and audit requirements, control agency audit requirements and, as necessary, disaster recovery requirements.
- **Logging.** All access to networked systems must be logged. When determined to be critical to the county, the logging of transactions must be included regardless of the operating platform. Log data must be classified as restricted. These logs must be retrievable through clearly defined procedures and must be maintained for time periods prescribed for audit, legal and recovery purposes. As new applications, platforms, mediums or other technical changes to system operations are made, consideration of logging requirements and availability must be made. Requirements for logging data must be clearly established as system, architectural, technical or network designs are developed.

Information Recovery

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

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

Data Exchange Agreements

- **Departmental Agreements.** Departments with systems that exchange data with/to any other entity must sign a formal agreement with that entity to adhere to specific agreed upon security protocols related to data exchange.
- **Third Party Agreements.** All agreements with third parties such as vendors, other government agencies, or contractors must include requirements to adhere to Clinton County's information security policies.

Vendor/Contractor Agreements

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

Employee/Agent Responsibilities

As a condition of continued employment, all employees/agents must sign an information security compliance agreement indicating that they have read and understand the county's policies and procedures regarding information security, and must agree to perform their work according to such policies and procedures.

- **Password Protection.** Employees/agents must not post or share their personal passwords, and must develop secure passwords not likely to be guessed.
- **Use of Automatic Logons.** Employees/agents must not facilitate any logon procedure with local programming such as keyboard programming or scripting.
- **Unattended Computers.** Unattended computers must be logged off or protected in such a way as to protect the computer and network from unauthorized access.

Reporting Suspicious Events. Any observations of suspicious activity must be reported to the appropriate county representative. Suspicious activity can include: signs of unauthorized equipment usage during evenings and weekends, phone requests from unidentifiable callers for access to secure information, unidentifiable files found on file servers, and unusual activity recorded in log files.