County of Clinton

# Information Technology Policies and Procedures

Rules and regulations for use of the
County of Clinton's
Network, Email and Internet

# Table of Contents

# 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 connection and services are provided for employees and approved interns, consultants, service providers and contractors performing business on behalf of a County agency/department (hereinafter referred to as County Information Technology Systems Users [County ITS Users]). The use of the Internet facilities by any County ITS User or other person authorized by the county must be consistent with this Acceptable Use Policy and the Information Technology Security Policy.

## 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 strong passwords. Accounts and passwords will be 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:

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

## 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 must have anti-virus software installed.
- 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 the Clinton County Information Technology Department. Other questions about appropriate use should be directed to your supervisor.

System administrators have access to all mail and user access requests, and will monitor messages as necessary to ensure efficient performance and appropriate use. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

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.

# Clinton County Government's
# Policy on Email Use

## Purpose and Goals

Email is one of Clinton County's core internal and external communication methods. The purpose of this policy is to ensure that Email systems used by County ITS Users 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 Email.

## Access to Email Services

Email services are provided to County ITS Users as resources allow. To request access, contact Clinton County Information Technology.

## Use of Email

Email services, like other means of communication, are to be used to support county business. County ITS Users may use Email to communicate informally with others in the county so long as the communication meets professional standards of conduct. County ITS Users may use Email to communicate outside of the county when such communications are related to legitimate business activities and are within their job assignments or responsibilities. County ITS Users **will not use** Email for illegal, disruptive, unethical or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interests of the County. The information communicated over agency Email systems is subject to the same laws, regulations, policies, and other requirements as information communicated in other written forms and formats.

## Privacy and Access

Email messages are **not** personal and private. Department Heads and Information Technology Staff may access an employee's Email:

- 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 Email when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.

Email 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** Email messages **including personal communications** may be subject to discovery proceedings in legal actions.

## Security

Email security is a joint responsibility of county technical staff and Email 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 Email Communications

Any Email message deemed a "business record" shall be archived and retained for as long as the law demands. A business record is any print or electronic document created in the normal course of official business and retained as evidence of official policies, actions, decisions or transactions.

Examples of messages sent by Email that typically are business records are:

- 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
- documents 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

Any Email message deemed a **Business Record** needs to be identified, managed, protected, and retained as long as 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 Email system** in accordance with the appropriate program unit's standard practices.

Business Records communicated via Email 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. The basic guidelines to follow when trying to decide if an Email and its attachments are records are to determine if they document the business of the government, decide what records series they belong in, and find what item in the appropriate schedule covers that series (refer to The University of the State of New York, The State Education Department, Records Retention and Disposition Schedule CO-2 formally adopted by the Clinton County Legislature – Resolution #251 dated 3/28/90). Most Email will be correspondence or memoranda, but related attachments may actually be reports, correspondence or a number of other kinds of records.

County ITS Users should:

- dispose of copies of records in Email 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 Email. 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 Information Technology staff** are responsible for Email security, backup and disaster recovery.

**All Email users** should:

- Be courteous and follow accepted standards of etiquette.
- Protect others' privacy and confidentiality.
- Consider organizational access before sending, filing, or destroying Email 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.

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 Email. 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 Information Technology staff are responsible for Email security, backup and disaster recovery.

## Policy Review and Update

The Information Technology Department 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 IT staff.

# County ITS Users Responsibilities

## User Access Management

Every user of the Clinton County network must have a network account.

- Each network account must be unique to each County ITS User and be created by the Information Technology Department.
- Network users who have multiple roles will be required to have a unique network account for each distinct role.
- Each network account will be set to disable access to the network for 24 Hours after 5 failed logon attempts.
- User accounts will be reviewed by the Information Technology Department every 90 days and will be audited by an internal audit.
- Network user accounts must not be shared between members of staff.
- Access to a County ITS Users account during absence by another member of the staff must be authorized by the Supervisor/Department Head.
- Unattended computers must be logged off or protected in such a way as to protect the computer and network from unauthorized access.

## Account Authentication

- All user accounts will be authenticated using passwords as a minimum.
- The minimum password length will be 8 characters.
- Each network password will be required to be changed at least every 90 days.
- Each network password will have a minimum life of 30 days.
- Complex passwords [consisting of 3 of 4--Upper case, lower case, numeric and non-alpha-numeric] must be used.
- Passwords cannot be reused for the next 4 times.
- Passwords for network accounts must not be shared unless an authorized shared account.
- Passwords must be stored encrypted.
- County ITS Users must not facilitate any logon procedure with local programming such as keyboard programming or scripting.

## New Network Accounts

- Clinton County exercises a formal user registration and deregistration process for all network users, permanent and temporary.
- All new accounts are to be requested by the department head 5 days before the employee starts, with all the required access specified.
- New accounts are created with a default password which the user is required to change at first logon.
- The initial password for a network user account will only be given to the new user or department head by phone or email.

## Account Changes / Removal

- Changes made to a network account (i.e. network access, email) must be submitted by the Department Head.
- Password resets must be requested by the network user of that account or their Supervisor/Department Head. Steps will be taken to verify the identity of the user.
- A locked account must be requested to be unlocked by that accounts user or their Supervisor/Department Head.

- All County ITS Accounts will be disabled if that user leaves their department. A deletion date will be entered into the disabled account 90 days from the disabled date.
- Notification of the account removal must be provided to the Information Technology Department a minimum of 5 days before the departure date.
- All network accounts that reach their deletion date will be deleted.
- Accounts used by staff on long term absence will be disabled, unless specified by the Department Head.

## 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.

## Downloading Software

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.) In addition, vendor copyright and licensing agreements must be strictly adhered to.

## 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.

## Virus Protection

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

## Account Review

- All network accounts will be reviewed after 7 days.
- Accounts that have not been used for 3 months will be automatically disabled.
- Unused accounts that have been disabled for 90 days will be deleted by the Information Technology Department.

## Account Types

## Network Administrator Accounts

- Network administrator accounts will be held and maintained by the Information Technology Department and corresponding positions.
- All activities of network administrator accounts will have audit logs enabled, giving a full audit trail of actions.

## User Accounts

- A user account is an account with standard user privileges and accessed by only one person at any one time.
- The privileges applied to user accounts must be only the minimum required for the role.

## Service / Application Accounts

- Service accounts are accounts which are not used by individuals but by applications to run services.
- Service accounts must be authorized by the Information Technology Department.
- Interactive logon should be disabled for service accounts.
- Passwords for Service Accounts must be recorded and stored securely.
- Application accounts give access to specific applications for which they have been created.
- Application accounts must comply with the account authentication rules wherever possible.
- Application accounts will be managed by the Information Technology Department.

As a condition of continued employment, all County ITS Users 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.

## 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.

# County of Clinton

## Clinton County's Information Technology Policies & Procedures Acknowledgement Form

By submitting and signing this form, I state that I have read, understood and have been given the opportunity to ask questions concerning the **Information Technology Network, Email and Internet Policies and Procedures** and the **Information Technology Security Policy** and agree to the terms and conditions of these policies. I understand that non-compliance with this agreement can result in immediate suspension of any or all network access as well as investigation, and/or referral for disciplinary action.

I also understand that logging and monitoring of computer usage may occur while alleged security breaches are being investigated.

I will not allow others to use my login or password. Staff requiring access to my files and mail in my absence should be trusted colleagues designated by my Department Head. They may be given delegate rights. If I am given delegate rights to another's information, I agree to respect that individual's right to confidentiality.

If I receive any suspicious, threatening or harassing material, or if I suspect that I might have received a virus, I will notify Information Technology.

Upon leaving Clinton County Government employment, I will notify the Information Technology Department immediately.

Print Name: _____

Signature: _____

Title: _____

Department: _____

Date: _____

*Please retain a copy of the Policy Statement for your files*.