CHAUTAUQUA COUNTY

Information Technology Policy

June 2021

Information Technology Department
Chautauqua County
Gerace Office Building
3 N. Erie St.
Mayville, New York 14757

Reference: Version 3.0

Guidelines Title: Information Technology Policy

Related Standards: Chautauqua County Identity Theft Prevention Policy, NYS Cyber Security Guidelines P03-002, NYS Information Classification and Control Guidelines and Standard PS08-001, NYS Cyber Security Citizens Notification Guidelines, New York State's Electronic Signatures and Records Act (ESRA) (9 NYCRR Part 540), State Certificate Guidelines for Digital Signatures and Encryption issued by the Office for Security, State Archive and Records Retention Administration (SARA), NYS Records Retention and Disposition Schedule CO-2, New York State Freedom of Information Act, Federal Rules of Civil Procedure, The Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH)

Replaces & Supersedes: Chautauqua County Computer Use Policy (**2016**)

Issued By: Jonathan DeAngelo
Chief Information Officer
Pursuant to Resolution 192-11

Revision Date: **June 2021**

Approved By: _____ **6/3/2021**
Paul Wendel Jr.
Chautauqua County Executive

Table of Contents

Information Security and Accountability

Preface

This Information Technology Policy is a statement of the minimum requirements, ethics, responsibilities and accepted behaviors required to establish and maintain a secure environment, and achieve the County's acceptable use and information security objectives. Compliance with these policies, guidelines and procedures is required and it is the responsibility of each County employee to ensure that they and their departments are in compliance.

Purpose

The purpose of this document is to ensure the confidentiality, integrity, and availability of computing resources by defining a set of minimum policies, guidelines and procedures that outlines the appropriate use, acquisition, and implementation that all Chautauqua County departments should strive to meet. This document applies to all Information Technology hardware, software, facilities, applications, and networks that are a part of Chautauqua County's computing resources and shall serve as best practices for the County, inclusive of all campus locations. Any department may, based on its individual business needs and specific legal requirements such as the Health Insurance Portability and Accountability Act (HIPAA), exceed the guidelines put forth in this document, but should, at a minimum, achieve the security levels outlined herein.

Scope

These policies, guidelines and procedures are applicable to County departments, staff and all others, including outsourced third parties, which have access to or manage County information. Where conflicts exist between these policies, guidelines and procedures and a County department guideline, the more restrictive guideline should take precedence.

Policy Monitoring and Enforcement

Computing systems and resources provided by Chautauqua County are owned by the County and are therefore its property. This gives Chautauqua County the right to monitor any and all voice, video, email, and all other data traffic passing through its system.

In addition, backup copies of voice, video, or data traffic may exist, despite end-user deletion, in compliance with Chautauqua County's records retention policy. The goals of these backup and archiving procedures are to ensure system reliability and prevent business data loss.

If Chautauqua County discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, voice, video, or data records may be retrieved and used to document the activity in accordance with due process.

.

Reporting Misuse

Any allegations of misuse should be promptly reported to your department head and the County Chief Information Officer. If you receive an offensive e-mail, do not forward, delete, or reply to the message. Instead, report it directly to the individuals named above.

Disclaimer

Chautauqua County assumes no liability for direct and/or indirect damages arising from an employee's use of Chautauqua County's voice, video, or data services. Employees are solely responsible for the content they disseminate. Chautauqua County is not responsible for any third-party claim, demand, or damage arising out of use of the County's voice, video, or data services.

Failure to Comply

Violations of any Information Technology Policy will be treated like other allegations of wrongdoing at Chautauqua County. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use on County voice, video, or data services may include, but are not limited to, one or more of the following:

- Temporary or permanent revocation of access to voice, video, or data resource; and/or
- Disciplinary action according to applicable County policies and collective bargaining agreements; and/or
- Legal action according to applicable laws.

Organizational Security and Functional Responsibilities

Information Owners

Chautauqua County departments are considered the information owners for the data and tools they administer. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, delete, archive, etc.). These access privileges should be in accordance with the user's job responsibilities.

County Employees

It is the responsibility of all employees to protect County information and resources, including passwords, and to report suspected security incidents to the appropriate manager and the County Information Security Officer. County employees are expected to adhere to the guidelines outlined in this document.

Non-County Employees

Individuals who work under the agreements with the County such as Contractors, Consultants, Vendors, interns, volunteers and other persons in similar positions, to the extent of their present or past access to County information, are also covered by this Information Technology Guidelines document.

Information Technology (IT)

Information Technology management has responsibility for the data processing infrastructure, data, voice, video, and wireless networks, that support the information owners. It is the responsibility of Information Technology management to support these policies, guidelines and procedures and provide resources needed to enhance and maintain a level of information security control that is consistent with this document.

Information Technology designated staff are responsible for the implementation of this and other acceptable use and information technology guidelines, but the compliance of County employees to these policies, guidelines and procedures is the Department Head's responsibility. The designated staff should educate County employees with regard to acceptable use and information security issues. Staff should be made aware of why the guidelines have been established, and what role(s) individuals have in safeguarding information.

Employee Information Security Policy Agreement

My signature below indicates that I have been provided with a copy of the Chautauqua County Information Technology Policy and I agree to abide by the policies and procedures explained herein. I understand it is my responsibility to read / review this policy and become familiar with this policy. If I violate any of the Information Security policies I may face legal or disciplinary action according to applicable laws, County policy, and/or collective bargaining agreements.

_____

Employee Name (Printed)

_____

Employee Signature Date

_____

Department

Acceptable Use Policies

CCIS- 0010.000 Policy - Email

Title	Number
Policy - Acceptable Use of Email	**CCIS-0010.000**
Creation Date: **September 2011**	
Modified Date: **June 2021**	

Purpose: E-mail is a critical mechanism for business communications at Chautauqua County. The objectives of this policy are to outline appropriate and inappropriate use of Chautauqua County's e-mail systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

Scope: This policy applies to all e-mail systems and services owned by Chautauqua County, all e-mail account users/holders at Chautauqua County (both temporary and permanent), and all County e-mail records.

General Policy: E-mail access at Chautauqua County is controlled through individual accounts and passwords. It is the responsibility of the employee to protect the confidentiality of their account and password information.

Employees of Chautauqua County are provided an e-mail account based on job function and business need as determined by the Department Head. E-mail accounts will be granted to third party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include contractors, vendors, and interns.

E-mail access will be terminated when the employee or third party terminates their association with Chautauqua County, unless other arrangements are made. Chautauqua County is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of their employment has ceased.

Chautauqua County's e-mail systems and services are not to be used for purposes that could be reasonably expected to cause excessive strain on systems. Individual e-mail use will not interfere with others' use of Chautauqua County's e-mail system and services.

The following activities are deemed inappropriate uses of Chautauqua County systems and services and are prohibited:

- Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
- Use of e-mail in any way that violates Chautauqua County's policies, rules, or administrative orders.

- Sending of unreasonably large e-mail attachments. The total size of an individual e-mail message sent (including attachment) should be 30 megabytes or less.
- Opening e-mail attachments or hyperlinks from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
- Sharing e-mail account passwords with another person, or attempting to obtain another person's e-mail account password. E-mail accounts are only to be used by the registered user.
- Excessive personal use of Chautauqua County e-mail resources. Chautauqua County allows limited personal use so long as it does not interfere with staff productivity. Chautauqua County prohibits personal use of its e-mail systems and services for unsolicited mass mailings, non-Chautauqua County commercial/for-profit activity, or political campaigning. The Chief Information Officer may restrict such personal use if necessary to conserve system resources for county purposes.

The e-mail systems and services used at Chautauqua County are owned by the County, and are therefore its property. This gives Chautauqua County the right to monitor any and all e-mail traffic passing through its e-mail system.

In addition, backup copies of e-mail messages may exist, despite end-user deletion, in compliance with Chautauqua County's records retention policy.

If Chautauqua County discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, e-mail records may be retrieved and used to document the activity.

Use extreme caution when communicating confidential or sensitive information via e-mail. Keep in mind that all e-mail messages sent outside of Chautauqua County become the property of the receiver.

Any allegations of misuse should be promptly reported to your immediate supervisor. If you receive an offensive e-mail, do not forward, delete, or reply to the message. Instead, report it directly to the individual named above.

Chautauqua County assumes no liability for direct and/or indirect damages arising from the user's use of Chautauqua County's e-mail system and services. Users are solely responsible for the content they disseminate. Chautauqua County is not responsible for any third-party claim, demand, or damage arising out of use the Chautauqua County's e-mail systems or services.

CCIS- 0020.000 Policy - Telephony Services

Title	Number
Policy - Acceptable Use of Telephony Services	**CCIS-0020.000**
Creation Date: **September 2011**	
Modified Date: **June 2021**	

Purpose: Telephone communication is an essential part of the day-to-day operations of Chautauqua County. Telephone and voicemail services are provided to employees in order to facilitate performance of work. The goal of this policy is to balance the business need for telephone and voicemail use with the costs involved.

Scope: This policy applies to all employees of Chautauqua County, and all usage of County provided telephone, voicemail and fax services.

General Policy: As with all Chautauqua County resources, the use of telephones, voicemail and fax services should be as cost effective as possible and in keeping with the best interests of the County. All employees must operate within the following basic policy guidelines:

- All telephones, telephony equipment, voicemail boxes, and messages contained within voicemail boxes are the property of Chautauqua County.
- The Information Technology Department is responsible for installation and repair of all County telephony equipment and administration of telephone and voicemail accounts with the exception of the Sheriff's Department e911 Dispatch Center.
- Department supervisors are responsible for overseeing telephone and voicemail use and ensuring policy compliance, as well as ensuring IT is notified of any adds, moves, or changes required to telephone or voicemail services.
- If you will be away from the office for more than one business day, you are expected to change your voicemail greeting to reflect this fact and direct callers to alternate contacts if applicable.

Unacceptable Use

Chautauqua County telephone, voicemail or fax services may not be used for the following:

- Transmitting obscene, profane, or offensive messages.
- Transmitting messages or jokes that violate the County's harassment policy or create an intimidating or hostile work environment.
- Using the telephone system or breaking into a voicemail box via unauthorized use of a PIN or other password.
- Broadcasting unsolicited personal views on social, political, or other non-business related matters.
- Soliciting to buy or sell goods or services unrelated to Chautauqua County.

- Making personal long-distance phone calls without supervisor permission and reimbursement.

Limited Personal Acceptable Use

In general, personal use of telephone, voicemail or fax services is allowable, but must be limited in number and duration and must not interfere with performance of official business duties. Limited personal acceptable use is allowed under the following circumstances:

- An employee's work schedule changes without advance notice and the employee must notify a family member or make alternate transportation or childcare arrangements.
- Brief local calls to a spouse, minor child, or elderly parent, or to those responsible for them (e.g. school, daycare center, nursing home).
- The employee needs to make a call that can only be made during regular working hours, such as to a doctor or local government agency.
- The employee needs to make arrangements for emergency repairs to his or her residence or automobile.
- A call that reasonably could not be made at another time and is of limited duration.

Monitoring

Chautauqua County reserves the right to monitor telephone, voicemail and fax use, including telephone conversations and the contents of voicemail boxes. Monitoring of telephone and voicemail use will only be done for legitimate reasons, such as to assess customer service quality assurance, retrieve lost messages, recover from system failure, or comply with investigations of wrongful acts.

CCIS- 0030.000 Policy - Cell Phones

Title	Number
Policy - Acceptable Use of Cell Phones	**Resolution 257-06**
Creation Date: **December 2006**	
Modified Date: **June 2021**	

Purpose: The purpose of this policy is to establish efficient and standard acceptable use policies with respect to cell phones.

Scope: This policy applies to all county issued mobile phones. This policy is to help ensure that this equipment is used for legitimate County business and serves a public purpose.

General Policy:

- Wireless telephones can be provided upon a department head or supervisor recommendation to any County employee to conduct only County business. The use of County wireless telephones for personal use is not permitted under any circumstance, except as defined in Paragraph (3) below. County mobile phones shall not be issued to non-County employees (i.e. contractors).
- In an emergency, extended work hours, unexpected travel, unscheduled overtime, or as allowed under union bargaining agreements, calls are not considered “personal” calls under the above prohibitions.
- Employees are responsible for taking proper care of wireless phones and reasonable precautions against damage, loss or theft. Loss of wireless phones should be reported to the supervisor and IT Department immediately. The employee shall replace losses attributed to negligence.
- Using a county-issued wireless phone while operating a motorized vehicle is strongly discouraged, and is strictly prohibited if not using proper hands-free equipment. With the exception of law enforcement officers and emergency services personnel in the case of emergency, employees are prohibited from using county-issued wireless phones while operating any motor vehicle, without proper hands free accessories.
- Wireless telephones are the property of Chautauqua County. No wireless telephone may be transferred to another department or worksite, or have changes in service ordered without the direct authority of a supervisor.
- All new wireless service and changes in existing wireless service must be ordered at the discretion of a supervisor.
- The county will periodically audit the usage of county-issued wireless phones.
- All County owned mobile phones must have secure access enabled (i.e. passcode, password).

CCIS- 0040.000 Policy - Mobile Devices

Title	Number
Policy - Acceptable Use of Mobile Devices	**CCIS-0040.000**
Creation Date: **September 2011**	
Modified Date: **June 2021**	

Purpose: The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data from a mobile device connected to an unmanaged network outside of Chautauqua County's direct control. The overriding goal of this policy is to protect the integrity of the private and confidential client and business data that resides within Chautauqua County's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored unsecured on a mobile device or carried over an unsecure network where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the County's public image.

Scope: The policy applies to any hardware and related software that could be used to access corporate resources, even if said equipment is not corporately sanctioned, owned, or supplied including

- Laptop/notebook/netbook/tablet computers.
- Mobile/cellular phones, air cards and GPS devices
- Smartphones, including but not limited to Apple iPhones\iPads, Android based devices, tablets, and other devices
- Home or personal devices used to access corporate resources.
- Any mobile device capable of storing corporate data and connecting to an unmanaged network.

All users employing a mobile device connected to an unmanaged network outside of Chautauqua County's direct control to backup, store, and otherwise access corporate data of any type must adhere to County-defined processes for doing so.

This policy applies to all Chautauqua County employees, including full and part-time staff, contractors, freelancers, and other agents who utilize either County-owned or personally-owned mobile device to access, store, back up, relocate or access any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust the County has built with its clients, supply chain partners and other constituents. Consequently, employment at Chautauqua County does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

Connectivity of all mobile devices will be centrally managed by Chautauqua County's IT department and will utilize authentication and strong encryption measures. Although IT is not able to directly manage external devices – such as home PCs – which may require connectivity to the corporate network, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the County's infrastructure.

General Policy: It is the responsibility of any employee of Chautauqua County who uses a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct County business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.

Based on this, the following rules must be observed:

- IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to the County infrastructure. IT will engage in such action if it feels equipment is being used in such a way that puts the County's systems, data, or users at risk.
- Laptop computers or personal PCs may only access the corporate network and data using a Virtual Private Network (VPN) or Remote Desktop Services (RDS) connection.
- All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any non-corporate computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by Chautauqua County's IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.
- In the event of a lost or stolen mobile device it is incumbent on the user to report this to IT immediately. The device will be remotely wiped of all data and locked if possible to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning.

CCIS- 0050.000 Policy - Internet

Title	Number
Policy - Acceptable Use of the Internet	
Creation Date: **September 2011**	
Modified Date: **June 2021**	

Purpose: The goals of this policy are to outline appropriate and inappropriate use of Chautauqua County's Internet resources.

Scope: Internet access at Chautauqua County is controlled through individual user accounts and passwords. Department managers are responsible for defining appropriate Internet access levels for the people in their department and conveying that information through a Help Desk Service Request ticket to the IT Help Desk.

General Policy:

Appropriate Use: Individuals at Chautauqua County are encouraged to use the Internet to further the goals and objectives of Chautauqua County. The types of activities that are encouraged include:

- Utilization of online applications directly related to job responsibilities;
- Acquiring information necessary or related to the performance of an individual's assigned responsibilities; and
- Participating in educational or professional development activities.

Inappropriate Use: Individual Internet use will not interfere with others' productive use of Internet resources. Internet use at Chautauqua County will comply with all Federal and New York State laws, all Chautauqua County policies, and all Chautauqua County contracts. This includes, but is not limited to, the following:

- The Internet may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, sexual harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, prohibited discriminatory activity, disruptive, unethical, unprofessional behavior and computer tampering (e.g. spreading computer viruses).
- The Internet may not be used in any way that violates Chautauqua County's policies, rules, or administrative orders. Use of the Internet in a manner that is not consistent with the mission of Chautauqua County, misrepresents Chautauqua County, or violates any Chautauqua County policy is prohibited.
- Excessive personal use of Chautauqua County Internet resources. Chautauqua County allows limited personal use so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources. Individuals should limit their personal use of the Internet to independent learning and public/community service. Internet access restrictions apply during times of personal use. Chautauqua County prohibits

personal use of its Internet resources and services for unsolicited mass mailings, non-Chautauqua County commercial/for-profit activity, political campaigning, dissemination of chain letters, and use by non-employees. The Chief Information Officer may restrict such personal use if necessary to conserve system resources for county purposes.

- Chautauqua County prohibits uploading and downloading of files for personal use without department head permission, and access to categories of sites (pornography, gaming, streaming media, etc.) as defined by access levels.
- Individuals may not establish County computers as participants in any peer-to-peer network file sharing programs, file transfer programs or listservs running on County information systems without consent from the CIO. Users shall not install internet software or programs unless authorized by the CIO or designee. Any unauthorized internet downloaded programs will be subject to removal by IT staff upon detection.

Security: For security purposes, users may not share account or password information with another person. Internet accounts are to be used only by the assigned user of the account for authorized purposes. Attempting to obtain another user's account password is strictly prohibited. A user must contact the help desk or IT administrator to obtain a password reset if they have reason to believe that any unauthorized person has learned their password. Users must take all necessary precautions to prevent unauthorized access to Internet services.

Monitoring and Filtering: Chautauqua County monitors all Internet activity occurring on Chautauqua County equipment or accounts. Chautauqua County currently does employ filtering software to limit access to sites on the Internet. If Chautauqua County discovers activities which do not comply with applicable law or departmental policy, records retrieved may be used to document the wrongful content in accordance with due process.

CCIS- 0060.000 Policy – Printers and Copiers

Title	Number
Policy – Acceptable Use of Printers and Copiers	**CCIS-0060.000**
Creation Date: **September 2011**	
Modified Date: **June 2021**	

Purpose: The goal of this policy is to facilitate the appropriate and responsible business use of printer and copier assets, as well as control the cost of ownership by preventing waste.

Scope: This Printer and Copier Policy applies to all employees of Chautauqua County as well as any contract employees in the service of the County who may be using this equipment.

General Policy:

- Printers and copiers are to be used for documents that are relevant to the day-to-day conduct of business at Chautauqua County. Printers and copiers should not be used to print personal documents.
- Installation of individual, non-shared printers is generally not condoned at Chautauqua County due to the cost of maintaining and supporting many dispersed machines. In certain circumstances, however, where confidentiality, remote location, the need to print a large number of low volume print jobs, or other unusual situation is at issue, personal printers may be allowed.
- If you print something to a common network attached printer / copier, please pick it up in a timely fashion. If you no longer want it, please dispose of it appropriately (i.e. recycle).
- Make efforts to limit paper usage by taking advantage of duplex printing (i.e. double-sided printing) features offered by some printers / copiers and other optimization features (e.g. printing six PowerPoint slides per page versus only one per page).
- Make efforts to limit toner use by selecting light toner and lower dpi default print settings.
- Avoiding printing a document just to see what it looks like. This is wasteful.
- Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper. If you need to use any of the paper types, consult with IT to find out which machines can handle these specialty print jobs.
- Color printing is typically not required by general business users. Given this selective need, as well as the high cost per page to print color copies, the number of color-capable printers available has been minimized. You are strongly encouraged to avoid printing in color when monochrome (black) will do.
- If you encounter a physical problem with the printer / copier (paper jam, out of toner, etc.) and are not “trained” in how to fix the problem, please do not try. Instead, report the problem to the IT Help Desk or ask a trained co-worker for help.

- Report any malfunction of any printing device to the IT Help Desk as soon as possible.

CCIS- 0070.000 Policy – Social Networks

Title	Number
Policy – Acceptable Use of Social Networks	**CCIS-0070.000**
Creation Date: **September 2011**	
Modified Date: **June 2021**	

Purpose: Social networking technologies can help support Chautauqua County business purposes. However, improper uses of such technologies raise security and network performance risks. The objective of this policy is to outline appropriate and inappropriate use of Social networking technologies in order to minimize disruptions to services and activities.

Scope: This policy applies to all social networking technologies that are accessed using a Chautauqua County email address, network access ID, or personal ID. Employees are responsible for their online activities that are conducted with any of these personal identities.

Employees should be aware that all Chautauqua County policies related to harassment, bullying, workplace violence, and ethics extend to all forms of communication (including social networking media) both inside and outside the workplace.

General Policy: A Chautauqua County employee may only use social networking technologies if authorized by his or her Department Head or supervisor, and the Director of Information Technology. Otherwise, accessing social networking technologies from a Chautauqua County computer is prohibited.

Appropriate Use: Upon approval, individuals are able to utilize social networking technologies to further the goals and objectives of Chautauqua County. Login identifications and passwords for maintenance of these sites should be shared with the department IT Liaison or Chief Information Officer. The types of activities that are encouraged include:

- Creation and monitoring of a social networking presence for a particular department such as the Health Department;
- Accessing social networking sites to gather information critical to public safety.

Inappropriate Use: Individuals shall not divulge sensitive or private information related to County operations or clients of any department whether operating on County sites, or personal sites. The types of activities that are forbidden include:

- Posting any information in violation of Federal, State, or County policies including (but not limited to) HIPAA, Identity Protection, and Workplace Violence. This applies whether the employee is utilizing a County account or a personal account.
- Divulging names, addresses, or other status or contact information about any County employee without consent of that employee, or any client of County services at any time.

Security Policies

CCIS- 0090.000 Policy – Network ID

Title	Number
Policy – Network ID and Password	**CCIS-0090.000**
Creation Date: **September 2011**	
Modified Date: **June 2021**	

Purpose: Passwords are an important component of information and network security. The use of a Network-ID and password combination serves to identify and authenticate a user to system resources and information assets. It is only through authenticated access that the enterprise can be assured that systems and data are being used appropriately. As such, passwords must be constructed, used and protected appropriately to ensure that the level of security they imply is actually met. The purpose of this policy is to provide the guidelines necessary for all of the employees of Chautauqua County to create appropriate passwords and to use them and protect them in an appropriate manner.

Scope: This policy applies to all employees of Chautauqua County who have any form of computer or application account that requires password access.

General Policy:

- Password construction, lifecycle and re-use parameters will be variable according to the application that they are intended to protect.
- Users will be notified in advance of county password expiration. Strong password construction is required and needs to be a minimum of fourteen characters in length, at least 1 capital letter and at least 1 number.
- Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell, or hint at their password to another person, administrators, superiors, other co-workers, friends, and family members.
- No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe or locked desk drawer if in hardcopy form or in an encrypted file if in electronic form.
- Each employee is responsible for all transactions made using his/her account.

CCIS- 0110.000 Policy – Removable Media

Title	Number
Policy – Removable Media	CCIS-0110.000
Creation Date: September 2011	
Modified Date: June 2021	

Purpose: The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to connect portable removable media to any infrastructure within Chautauqua County's internal network(s) or related technology resources. This removable media policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives.
- Memory cards in SD, CompactFlash, Memory Stick, or any related flash-based supplemental storage media.
- USB card readers that allow connectivity to a PC.
- Devices with internal flash or hard drive-based memory that support a data storage function including cellular phones.
- Digital cameras with internal or external memory support.
- Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks.
- Any hardware that provides connectivity to USB devices through means such as wireless (WiFi, WiMAX, irDA, Bluetooth, among others) or wired network access.

Scope:

The policy applies to any hardware and related software that could be used to access County resources, even if said equipment is not corporately sanctioned, owned, or supplied.

General Policy: It is the responsibility of any employee of Chautauqua County who is connecting a USB-based memory device to the organizational network to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any portable memory that is used to conduct Chautauqua County business be utilized appropriately, responsibly, and ethically.

Based on this, the following rules must be observed:

- By default, and enforced by software policy where possible, the use of removable media will not be permitted. Chautauqua County's IT department will support approved media on a case-by-case basis, and is not accountable for conflicts or problems

caused by the use of unsanctioned media. This applies even to devices already known to the IT department.

- IT reserves the right to physically disable USB ports to limit physical and virtual access and reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

CCIS- 0120.000 Policy – Anti-Virus and Malware

Title	Number
Policy – Anti-Virus and Malware	CCIS-0120.000
Creation Date: September 2011	
Modified Date: June 2021	

Purpose: A virus or malware is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses or malware can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, and other media.

As a result, one of the goals of Chautauqua County is to provide a computing network that is virus and malware free. The purpose of this policy is to provide instructions on measures that must be taken by Chautauqua County employees to help achieve effective virus and malware detection and prevention.

Scope: This policy applies to all computers that are connected to the Chautauqua County network via a standard network connection, wireless connection, or virtual private network connection. This includes both County-owned computers and personally-owned computers attached to the County's network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, smart phones and servers.

General Policy: All computers attached to the County's network must have anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

Any activities with the intention to create and/or distribute malicious programs onto the County network are strictly prohibited.

If an employee receives what he/she believes to be a virus or malware, or suspects that a computer is infected with a virus, must contact the IT department immediately and report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT department.

Any virus or malware infected computer will be removed from the network until it is verified as virus or malware free.

CCIS- 0130.000 Policy – Third Party Access

Title	Number
Policy – Third Party Access	**CCIS-0130.000**
Creation Date: **September 2011**	
Modified Date: **June 2021**	

Purpose: The purpose of the Chautauqua County Third-Party Access Policy is to establish the rules for third-party access to County information systems, third-party responsibilities, and protection of Chautauqua County information.

Scope: The Chautauqua County Third-Party Access Policy outlines responsibilities and expectations of any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. This policy also outlines the responsibilities and expectations of the County personnel responsible for the contracting and/or supervising of the third party. A third party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and security companies.

General Policy:

Information Systems Third-Party Policy Guidelines

- Any third-party agreements and contracts must specify:
    - The work that is to be accomplished and work hours. Also, any configuration information of any installed software as well as virus checking of that software.
    - The information that the third party requires access to.
    - The minimum security requirements that the third party must meet (i.e. method for remote access).
    - How County information is to be guarded by the third party. Signing of a business associate agreement may be required.
    - Strict use of County information and information resources for the purpose of the business agreement by the third party. Any other County information acquired by the third party in the course of the contract cannot be used for the third-party's own purposes or divulged to others.
    - Feasible methods for the destruction, disposal, or return of County information at the end of the contract.
    - The return of County property such as a laptop after the completion or termination of the agreement.
- The third party must comply with all applicable Chautauqua County standards, agreements, practices and policies, including, but not limited to:

- Acceptable use policies.
- Software licensing policies.
- Safety policies.
- Auditing policies.
- Security policies.
- Non-disclosure policies.
- Privacy policies.

- Chautauqua County will provide an IT point of contact for the third party whether it is one person from the IT department or an interdepartmental team. This point of contact will communicate with the third party to ensure they are in compliance with these policies.
- The third party will provide the County with a list of all additional third parties working on the contract. The list must be updated and provided to the County within 8 hours of any staff changes.
- Third party access to systems must be uniquely identifiable and authenticated, and password management must comply with the Chautauqua County Password Policy. Managing connectivity with partner networks can be handled different ways depending on what technologies are in place (i.e. encryption, intrusion detection, DMZ architecture).
- Any third party computer that is connected to County systems must have up-to-date virus protection and patches. The third party will be held accountable for any damage occurred to the County in the event that an incident occurs.
- Third-party employees must report all security incidences to the appropriate County Information Technology Department personnel.
- If third-party management is involved in Chautauqua County security incident management, the responsibilities and details must be specified in the contract.
- The third party must follow all applicable change control procedures and processes.
- All software used by the third party in providing service to Chautauqua County must be properly inventoried and licensed.
- All third-party employees are required to comply with all applicable auditing regulations and County auditing requirements, including the auditing of the third-party's work.
- All third-party maintenance equipment on the County network that connects to the outside world via telephone lines, leased line, or the network will remain disabled except when in use for authorized maintenance.

- Upon departure of the third party from the contract for any reason, the third party will ensure that all sensitive information is collected and returned to the County or destroyed within 72 hours. The third party will also provide written certification of that destruction within 5 business days. All equipment and supplies must also be returned, as well as any access cards and identification badges. All equipment and supplies retained by the third party must be documented by authorized County management.

Communications and Network Management Policies

CCIS- 0150.000 Policy – Remote Access

Title	Number
Policy – Remote Access	**CCIS-0150.000**
Creation Date: **September 2011**	
Modified Date: **June 2021**	

Purpose: The purpose of this policy is to define standards, procedures, and restrictions for connecting to Chautauqua County's internal network(s) from external hosts via remote access technology, and/or for utilizing the Internet for business purposes via third-party wireless Internet service providers (a.k.a. "hotspots"). Chautauqua County's resources (i.e. county data, computer systems, networks, databases, etc.) must be protected from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all remote access and mobile privileges for County employees to enterprise resources – and for wireless Internet access via hotspots – must employ only County-approved methods.

Scope: This policy applies to all Chautauqua County employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who utilize County- or personally-owned computers to remotely access the organization's data and networks. Employment at Chautauqua County does not automatically guarantee the granting of remote access privileges.

Any and all work performed for Chautauqua County on said computers by any and all employees, through a remote access connection of any kind, is covered by this policy. Work can include (but is not limited to) e-mail correspondence, Web browsing, utilizing intranet resources, and any other County application used over the Internet. Remote access is defined as any connection to the County's network and/or other applications from off-site locations, such as the employee's home, a hotel room, airports, cafés, satellite office, wireless devices, etc.

All remote access will be centrally managed by Chautauqua County's Information Technology department and will utilize encryption and strong authentication measures.

Employees may use privately owned connections for business purposes. However, the County's IT department cannot and will not technically support a third-party ISP connection.

General Policy: It is the responsibility of any employee of Chautauqua County with remote access privileges to ensure that their remote access connection remains as secure as his or her network access within the office. It is imperative that any remote access connection used to conduct Chautauqua County business be utilized appropriately, responsibly, and ethically. Therefore, the following rules must be observed:

- Employees will use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with the County's password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

- All remote computer equipment and devices used for business interests, whether personal- or County-owned, must display reasonable physical security measures. Computers will have installed whatever antivirus software deemed necessary by Chautauqua County's IT department.
- Remote users using public hotspots for wireless Internet access must employ for their devices a County-approved personal firewall, VPN, and any other security measure deemed necessary by the IT department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with Chautauqua County's additional security measures.
- Any remote connection that is configured to access Chautauqua County resources must adhere to the authentication requirements of the County's IT department. In addition, all hardware security configurations (personal or County-owned) must be approved by Chautauqua County's IT department.
- Employees, contractors, and temporary staff will make no modifications of any kind to the remote access connection without the express approval of the County's IT department. This includes, but is not limited to, split tunneling, dual homing, non-standard hardware or security configurations, etc.
- Employees, contractors, and temporary staff with remote access privileges must ensure that their computers are not connected to any other network while connected to Chautauqua County's network via remote access, with the obvious exception of Internet connectivity.
- In order to avoid confusing official County business with personal communications, employees, contractors, and temporary staff with remote access privileges must never use non-County e-mail accounts (e.g. Hotmail, Yahoo, etc.) to conduct Chautauqua County business. Remote connections should be terminated as soon as official County business is completed.
- If a personally- or County-owned computer or related equipment used for remote access is damaged, lost, or stolen, the authorized user will be responsible for notifying their manager and Chautauqua County's IT department immediately.
- The remote access user also agrees to immediately report to their manager and the County's IT department any incident or suspected incidents of unauthorized access and/or disclosure of County resources, databases, networks, etc.
- The remote access user also agrees to and accepts that his or her access and/or connection to Chautauqua County's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

CCIS- 0160.000 Policy – Wireless Networks

Title	Number
Policy – Wireless Networks	**CCIS-0160.000**
Creation Date: **September 2011**	
Modified Date: **June 2021**	

Purpose: The purpose of this policy is to outline appropriate and inappropriate use of Chautauqua County's Wireless Networking resources, including

- Devices that are permitted to connect to the wireless network
- Access privileges for the wireless network (i.e. who is authorized and who is not authorized to use the wireless network)
- Consequences for violating the wireless networking policy.

Scope: Only County owned and approved wireless devices are permitted to connect to the wireless network. The IT department is responsible for approving wireless devices for use on the network. In certain situations, non-county owned devices may be permitted to connect to the wireless network. The IT department must approve each of these situations in advance.

General Policy: The IT department is responsible for setting standards for hardware, software, and other technology that will be used in the wireless network. Only the Information Technology Department is authorized to attach wireless hubs or switches (commonly known as Access Points or AP's) to the Chautauqua County cabled network.

User-owned equipment will not necessarily be in compliance with corporate standards, and may not be supported by the IT department. Users should contact the IT department to discuss any issues relating to wireless networking technology standards.

The IT department is responsible for granting access privileges to the wireless network. The County may provide public access to the Internet in some locations.

All users accessing the wireless network must comply with County security policies.

The wireless network(s) provided by the County shall be utilized for County business only. Employees, contractors, and others shall not utilize County wireless network resources for personal use.

.

CCIS- 0200.000 Policy – Software Use/Licensing

Title	Number
Policy – Software Use/Licensing	**CCIS-0200.000**
Creation Date: **September 2011**	
Modified Date: **June 2021**	

Purpose: Chautauqua County believes in respecting and protecting the rights of intellectual property owners. This is not only a question of ethics, but also of law.

Scope: The goal of this policy is to inform employees at Chautauqua County on rules and procedures relating to copyright law compliance and valid licensing, and pertains to any and all County owned equipment and resources that are connected to the County network.

General Policy:

- Chautauqua County reserves the right to monitor end-user systems and the content stored therein. Chautauqua County also reserves the right to remove, delete, modify, or otherwise disable access to any materials found to be infringing on copyright, valid licensing or unauthorized installations or downloads.
- By reading and signing a copy of this policy, an employee of Chautauqua County will indemnify and hold Chautauqua County harmless for any breach of this policy or copyright law.
- No employee of Chautauqua County may reproduce any copyrighted work in violation of the law. Unauthorized copying material includes but is not limited to, digitization, graphics, distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, movies, logos, and the installation of any "pirated" or other copyrighted or unlicensed software products for which the County does not have an active appropriate license, is strictly prohibited. All software acquired must be reviewed and purchased through the Information Technology Department. Under no circumstances will personal or unsolicited software be loaded onto County computers. Users are not permitted to bring software from home (or any other external source) and load it onto County computers. Users are not permitted to install programs from the internet, including freeware or shareware unless reviewed and authorized by the County Information Technology Department. Every piece of software is required to have a license and Chautauqua County will not condone the use of any software that is not licensed. Unauthorized changes to software must not be made. Copying and reproducing County owned or licensed software for personal use is strictly prohibited.

Contact Information

Questions concerning this guideline or requests for changes may be directed to:

Director of Information Technology
Information Technology Department
Chautauqua County
Gerace Office Building
3 North Erie St
Mayville, New York 14757
716-753-4281