INFORMATION TECHNOLOGY POLICY

COUNTY OF AROOSTOOK

SEPTEMBER 21, 2022

BRYAN V. JANDREAU, FACILITIES & IT DIRECTOR

INFORMATION TECHOLOGY SERVICE PROVIDER
ROBERT SOWERS, OAK LEAF SYSTEMS, INC.

County of Aroostook - Information Technology Policy

INDEX

County of Aroostook
INFORMATION TECHOLOGY POLICY

Subject: INFORMATION TECHOLOGY POLICY

Approved by the Board of Aroostook County Commissioners:

Signed in minutes
Paul J. Adams

Signed in minutes
Norman L. Fournier

Signed in minutes
Paul J. Underwood

Effective Date: 02/15/2023

1 Notation

This information technology policy shall work in conjunction with the County of Aroostook Personnel Policy Manual; including its Section XXV, Email and Internet Usage, pages 48-51. (Appendix A) Personnel Policy Manual, XXV. Email & Internet Use.

2 Acronym

- The use of the term/acronym "COA" is in reference to the following organization: County of Aroostook.
- The use of the term/acronym "IT" is in reference to: Information Technology.

3 Scope

This policy applies to all employees (hired, appointed and elected) and third parties with access to COA electronic information resources.

4 Devises and Platforms

This policy applies to all communication devises and platforms consisting of, but not limited to, telephone, fax, radio, pc, laptop, note book, note pad, cellular phone, email, email attachment, chatting, texting, instant messaging, website contact us, and social media.

5 Introduction

This policy is a formal set of rules by which those who are given access to COA technology and information assets must abide.

This policy serves several purposes. The main purpose is to inform COA users: employees (elected, hired and appointed), contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of the COA. The information technology security policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.

This policy also describes the user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The policy answers these questions, describes user limitations and informs users there will be penalties for violation of the policy. This policy also contains procedures for responding to incidents that threaten the security of the COA computer systems and network.

6 Protection

It is the obligation of all users of the COA systems to protect the technology and information assets of the COA. This information must be protected from unauthorized access, theft and destruction. The technology and information assets of the COA are made up of, but not limited to, the following components:

- Computer hardware, CPU, disc, thumb-drive, email, web, application servers, PC systems, switches, voicemail servers, cellular phones, radios, telephones, fax machines, application software, etc.
- System Software including operating systems, database management systems, and backup and restore software, communications protocols, and so forth.

- Application Software: used by the various departments within the COA. This includes custom written software applications, and commercial off the shelf software packages.
- Communications Network hardware and software including routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

7 Ownership/Property

All data within the COA information technology system is owned by the COA. Proprietary data from third parties used by the COA are used through agreement/contract between the third party and the COA and NOT between an employee of the third party and an employee of the COA.

8 Threats to Security

8.1 Employees

Some of the biggest security threats often come from within an organization, whether in be from a lack of system understanding or on purpose. Security is to be layered to compensate for that by doing the following.

- Only give out appropriate rights to systems.
- Do not share accounts to access systems. Never share login information with co-workers.
- When employees are separated or disciplined, remove or limit access to systems as appropriate.
- Physically secure computer assets, so that only staff with appropriate need can access.

8.2 Amateur Hackers

Amateur hackers are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be a large number of attacks. These are usually crimes of opportunity. These amateur hackers scan the Internet looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favorite targets. Once they find a weakness they will exploit it to plant viruses, Trojan horses use the resources of your system for their own means. If they do not find an obvious weakness, they are likely to move on to an easier target. It is helpful for all employees to be aware that this type of activity exists and can be a threat to our information technology systems.

8.3 Criminal Hackers

The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network. It is helpful for all employees to be aware that this type of activity exists and can be a threat to our information technology systems.

9 User Responsibilities

This section establishes usage policy for computer systems, networks and information resources of the COA. It pertains to all employees (elected, hired and appointed) and contractors who use the computer systems, networks, and information resources as business partners, and individuals who are granted access to the network for the business purposes of the COA.

9.1 Acceptable Use

User accounts on COA computer systems are to be used only for business of the COA and not to be used for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and can be punishable by law. Therefore, unauthorized use of the COA computing system may constitute grounds for either discipline, dismissal, civil or criminal prosecution.

Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore, they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons of the COA or outside of the COA.

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to COA systems for which they do not have authorization.

Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the employees' supervisor and/or the COA IT designee.

Users shall not download unauthorized software from the Internet onto their PCs or workstations. Software downloads shall be preapproved by the COA IT designee.

Users are required to report any weaknesses in the COA computer system, any incidents of misuse or violation of this policy to their immediate supervisor.

9.2 Use of the Internet

The COA will provide Internet access to employees and contractors who are connected to the internal network and who have a business need for this access. Employees and contractors must obtain permission from their supervisor and obtain authorization from the COA IT designee for such access.

The Internet is a business tool for the COA. It is to be used for business-related purposes such as: communicating via electronic mail with suppliers and business partners, obtaining useful business information and relevant technical and business topics.

The Internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature, chain letters or any other purpose which is illegal or for personal gain.

9.3 Monitoring Use of Computer Systems

The COA has the right and capability to monitor electronic information created and/or communicated by persons using COA computer systems and networks, including e-mail messages and usage of the Internet. It is not the COA policy or intent to continuously monitor all computer usage by employees or other users of the COA computer systems and network. However, users of the systems should be aware that the COA may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g., site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with COA policy.

10 Access Control

A fundamental component of our information technology policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements. Examples of COA applications and databases are Munis, ICON, Brown Tech, COA website, etc.

10.1 User System and Network Access

All users will be required to have a unique logon ID and password for access to systems, E.g. Munis, E-mail; voice mail, ICON, Brown Tech, etc. The user's password should be kept confidential and MUST NOT be shared with management & supervisory personnel and/or other employees. All users must comply with the following rules regarding the creation and maintenance of passwords:

- Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.

Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file on any computer system is prohibited. Password management shall be the duty of the COA IT designee.

Employee logon IDs and passwords will be deactivated as soon as possible if the employee is terminated, suspended, placed on leave, or otherwise leaves the employment of the COA.

Supervisors/Managers shall immediately and directly contact the COA IT designee to report change in employee status that requires terminating or modifying employee logon access privileges.

Employees who forget their password must call the COA IT designee to get a new password assigned to their account.

Employees will be responsible for all transactions occurring during logon sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer/system and then allow another individual to use the computer/system or otherwise share access to the computer systems.

10.2 System Administrator Access

The COA IT designee and the COA IT service contractor shall have administrative access, but not limited to, host systems, routers, hubs, and firewalls as required to fulfill the duties of their job.

All system administrator passwords will be ***DELETED*** immediately in the event that the COA IT designee and/or the COA IT service contractor is terminated, fired, or otherwise leaves the employment or services of the COA.

10.3 Connecting to Third-Party Networks

This policy is established to ensure a secure method of connectivity provided between the COA and all third-part companies and other entities required to electronically exchange information with the COA.

"Third-party" refers to vendors, consultants and business partners doing business with the COA, and other partners that have a need to exchange information with the COA. Third-party network connections are to be used only by the employees of the third-party, only for the business purposes of the COA. The third-party company will ensure that only authorized users will be allowed to access information on the COA network. The third-party will not allow Internet traffic or another private network traffic to flow into the network. A third-party network connection is defined as the following:

- A network connection will terminate on a (per session use/need) and the third-party will be subject to standard COA authentication rules.

This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed.

All requests for third-party connections must be made by submitting a request and be approved by the COA.

- Public Wi-Fi provided by COA that is separated from the COA network shall be the preferred method of connectivity for a third-party.

10.4 Connecting Devices to the Network

Only authorized devices may be connected to the COA network(s). Authorized devices include PCs and workstations owned by COA that comply with the configuration guidelines of the COA. Other authorized devices include network infrastructure devices used for network management and monitoring.

Users shall not attach to the network: non-COA computers that are not authorized, owned and/or controlled by the COA. Users are specifically prohibited from attaching (gaming devices) to the COA network.

NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the network or any unauthorized storage devices, e.g. thumb drives and writable CD's that are not the property of the COA.

10.5 Remote Access

Only authorized persons may remotely access the COA network. Remote access is provided to those employees, contractors and business partners of the COA that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the network or a remote network to COA network connection.

- COA remote connectivity shall be done so by a COA virtual private network (VPN).

10.6 Unauthorized Remote Access

The attachment of (e.g. hubs) to a user's PC or workstation that is connected to the COA WAN is not allowed without the permission of the COA. Additionally, users may not install personal software designed to provide remote control of the PC or workstation without the permission of the COA. This type of remote access without the appropriate protocols in place bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

11 Penalty for Policy Violation

The COA takes the issue of information technology seriously. Persons who use the technology and information resources of the COA must be aware that they can be disciplined if they violate this policy. Upon violation of this policy, an employee of the COA (hired, appointed and elected) may be subject to discipline up to and including dismissal. The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of the information technology policy, prior violations of the policy committed by the individual, state and federal laws and all other relevant information. Discipline which may be taken against an employee shall be administrated in accordance with any appropriate rules or policies and the COA Personnel Policy Manual.

In a case where the accused person is not an employee of the COA, the matter shall be submitted to the County Administrator. The County Administrator may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

12 Tik Tok

This policy prohibits the installation and use of Tik Tok on County of Aroostook (COA) devices. Personal devices that have Tik Tok installed are prohibited from connecting to the COA network.

The COA must keep pace with a rapidly evolving cyber threat landscape that poses significant risks to the security of the County's network infrastructure, including the sensitive and confidential data that we are entrusted to protect for our citizens. This policy is in response to well-documented national security risks posed by TikTok, a Chinese-owned video-sharing mobile application, recently enacted federal legislation and State of Maine gubernatorial directive that prohibits the use of the application on all federal and state government devices. (Effective 02/15/2023).

APPENDIX A – Personnel Policy Manual, XXV. Email & Internet Usage

XXI. E-MAIL & INTERNET USAGE

E-mail is for business use, not personal use. It is property of Aroostook County Government. The Aroostook County Government may from time to time examine e-mail or other computer files or documents of any employee within the organization. For this reason, employees should not commit anything to e-mail which is so personal or private that they would not wish others to see it. E-mail is not to be used to solicit others for commercial or non-commercial purpose including, but not limited to, bake sales, Girl Scout cookies, Tupperware, charities, social, political or other purposes.

All County employees required to use a computer and email for County business will be required to use the County email address assigned to the employee. This email address will be used for County business and is the property of Aroostook County Government.

Internet access to global electronic information resources on the World Wide Web is provided by the Aroostook County Government to assist employees in obtaining work-related data and technology. The following guidelines have been established to help ensure responsible and productive Internet usage.

All Internet data that is composed, transmitted, or received via our computer communications systems is considered to be part of the official record of the Aroostook County Government and, as such, is subject to disclosure to law enforcement or other third parties. Consequently, employees

should always ensure that the business information contained in Internet email messages and other transmissions is accurate, appropriate, ethical, and lawful.

The equipment, services, and technology provided to access the Internet remain at all times the property of the Aroostook County Government. As such, the Aroostook County Government reserves the right to monitor Internet traffic, and retrieve and read any data composed, sent, or received through our online connections and stored in our computer systems.

Data that is composed, transmitted, accessed, or received via the Internet must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, sexual orientation, religious beliefs, national origin, disability, or any other characteristic protected by law.

The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited. As a general rule, if an employee did not create material, does not own the rights to it, or has not gotten' authorization for its use, it should not be put on the Internet.
Employees are also responsible for ensuring that the person sending any material over the Internet has the appropriate distribution rights.
Internet users should take the necessary anti-virus precautions before downloading or copying any file from the Internet. All downloaded files are to be checked for viruses; all compressed files are to be checked before and after decompression.

Abuse of the Internet access provided by the Aroostook County Government in violation of law or the Aroostook County Government policies will result in disciplinary action, up to and including termination of employment. Employees may also be held personally liable for any violations of this policy. The following behaviors are examples of previously stated or additional actions and activities that are prohibited and can result in disciplinary action:

• Sending, forwarding or posting discriminatory, harassing, or threatening messages or images;
• Stealing, using, or disclosing someone else's code or password without authorization;
• Violating copyright law;
• Failing to observe licensing agreements;
• Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions;
• Sending, forwarding or posting discriminatory, harassing, or threatening messages or images;
• Stealing, using, or disclosing someone else's code or password without authorization;
• Violating copyright law;
• Failing to observe licensing agreements;

• Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions;
• Sending, forwarding or posting messages or material that could damage the organization's image or reputation;
• Participating in the viewing or exchange of pornography or obscene materials;
• Sending, forwarding or posting messages that defame or slander other individuals;
• Sending, forwarding or posting chain letters, solicitations, or adve1tisements not related to business purposes or activities;
• Using the Internet for political causes or activities, religious activities, or any sort of gambling;
• Jeopardizing the security of the organization's electronic communications systems;
• Sending anonymous email messages;
• Engaging in any illegal activities;
• Engaging in social networking sites such as, but not limited to Myspace, Facebook, etc., for personal use during work time and using the County's computer equipment.

APPENDIX B – Review of this Policy

DATE	PAGE	CHANGE	NOTES
02/15/2023	*9 #12*	Tik Tok Policy	Added to policy
13/17/2023	*INDEX*	Review Section	Added to Index
03/17/2023	12 Appx B	Review Section	Added to policy

[END OF POLICY]