Anoka County
COUNTY ADMINISTRATION
Information Technology

Anoka County

Technology Security Policy

Anoka County

Adopted: December 10, 2007 Revised: August 22, 2017

TECHNOLOGY SECURITY POLICY

Table of Contents

TECHNOLOGY SECURITY POLICY

1.0 Introduction

The use of technology resources permeates our everyday work life. When used properly, our technology resources greatly enhance our job productivity and efficiency. This security policy sets out rules and umbrella guidelines that can be used in the protection of our data and technology resources, and serves as the foundation for the County's technology security infrastructure. This document addresses the security of our technical infrastructure, and the expected behavior of the users of our electronic systems. It is your responsibility to secure and protect the information you access as a part of your job.

Ensuring the security of the County's technology resources is critical to maintaining the confidentiality, integrity, and availability of our data and other electronic information assets.

This Technology Security Policy serves to:

- Ensure proper accountability and protection of any electronic information related to County business;
- Maintain controls necessary for the County to operate efficiently;
- Enable greater productivity for our users;
- Comply with Federal and State law and Anoka County policies; and
- Document a comprehensive county-wide standard for security planning and execution

Managing Risk

It is impossible to eliminate all risk. Therefore, security measures will be taken to reduce risk to a reasonable and appropriate level to ensure the confidentiality, integrity and availability of all electronic data created, received, disseminated or maintained by Anoka County. With all security decisions, it is important to keep in mind what can be done to reduce risk to an acceptable level, given the criticality of the outcome and the limitations faced. Keeping the risk of the outcome in mind will help to formulate decisions about the level of security required for an electronic information asset.

Acceptable risk will be defined through identifying the County's technology risk exposures, examining the various alternatives to either eliminate or reduce those exposures, selecting the appropriate alternative(s) to deal with each risk, implementing the most feasible alternative(s), and monitor the alternative(s) for the purpose of altering or improving the risk exposure.

Securing our Information

Technology resources are exposed to multiple threats and therefore, securing our resources must include administrative, technical and physical safeguards to protect against these threats. For example, our security environment includes the use of such measures as firewalls, encryption, passwords, anti-virus software, and physical locks, just to name a few. User awareness and protection is another layer of defense that is important to our security protection. Please always keep security in mind in the use of your technology resources.

2.0 Purpose

This policy documents a comprehensive County-wide standard for technology security planning and execution to ensure that the County's electronic information assets are protected against destruction, theft, loss, unauthorized access, unauthorized change, and disruption of service. This policy shall serve as a foundation for

TECHNOLOGY SECURITY POLICY

the County's technology security infrastructure in accordance with the Anoka County Personnel Rules and Regulations, the Anoka County HIPAA Policies the Anoka County Data Policies, and describes the required actions to ensure the security of technology resources. Each County division, department, and office should align specific security requirements, programs, processes, and procedures in accordance with this policy and based on their business needs.

Technology is ever-changing and never static. Accordingly, security practices and policies must be adapted to those changes. This policy was created to be applicable to the County's changing needs and security requirements.

The Anoka County Technology Security Policy Supporting Documents has been designed as a supplement to this policy in order to address changes in technology and security specific terminology, infrastructure standards, password guidelines, incident reporting, and associated technology usage agreements for County employees and vendors. The Anoka County Board of Commissioners authorizes the Director of Information Technology to routinely make modifications or updates to the Technology Security Policy Supporting Documents in order to protect Anoka County's electronic information assets.

The Technology Security Policy is intended to protect the confidentiality, integrity, and availability of our data and other electronic information assets, wherever they may reside or however they are accessed. Due care must be exercised to appropriately protect the County's electronic information from origin to destination, both internal and external to the County information systems and networks.

Security is critical to the success of technology initiatives and acquisitions. Each technology project must include a security review to ensure that policies are followed and electronic information assets are protected. Each County division, department, and office is responsible for defining their specific security requirements, documenting procedures, and implementing appropriate security processes in support of this Technology Security Policy and other documented guidelines. The Department of Information Technology, in conjunction with County divisions, departments, and offices will provide security training and education to County employees and vendors to facilitate security awareness throughout the County.

Anoka County strives to keep private, confidential and not-public data private and confidential while ensuring transparency and public access to all public data. Pursuant to Minnesota Statute Section 13.05 subd. 5 and Administrative Rule 1205.044 subpart 2, it is the policy of Anoka County that its employees do not access private, confidential or not-public records or information unless their work assignments reasonably require access to such records. The ability of authorized individuals to enter, update, or access data is limited through the use of role-based access that corresponds to the official duties or training level of the individual as assigned by that employee's supervisor. Unauthorized access may result in discipline up to and including termination as well as potential criminal sanctions.

TECHNOLOGY SECURITY POLICY

2.1 Objectives

This policy includes the following objectives:

- Ensuring the safe keeping of electronic information assets;
- Establishing county-wide standards of acceptable behavior for information security;
- Creating a reference document to be used for establishing information security controls, compliance, and incident reporting;
- Assisting with meeting legal and authoritative regulations;
- Protecting electronic data and information integrity, confidentiality and availability; and
- Providing security enforcement mechanisms.

2.2 Scope

This policy covers all Anoka County electronic information assets supported or maintained by the Department of Information Technology, and applies to all employees, vendors, contractors and officials of Anoka County.

2.3 Authority and Compliance

All County employees, vendors, contractors, officials or other personnel using county electronic information assets as defined in §1.2 Scope, are responsible for complying with this policy and any related guidelines, procedures and processes. Anyone becoming aware of violations of this policy must immediately report the violation to their immediate supervisor. The supervisor shall notify Risk Management and the Help Desk.

Failure of an employee to comply with any of the provisions of this policy shall be considered Just Cause for discipline under the Anoka County Personnel Rules and Regulations, any Union Contract or Employment Agreement then existing between the County and the employee up to and including termination of County employment.

Use of any outside vendor, Application Service Provider (ASP), partnership, consortium or alliance for processing of electronic information, must be monitored and reviewed by the responsible County division, department, or office to ensure compliance with this policy, and any related guidelines. This will be accomplished through contractual commitments with provisions to permit auditing and monitoring to ensure compliance.

2.4 Contingency Planning

These policies have been developed in conjunction with on-going disaster recovery planning. Information assets considered critical, essential, urgent, necessary or important to County operations must include a detailed disaster recovery plan to minimize impact disruption or unavailability. County divisions, departments, and offices must also ensure that alternative business plans have been developed and implemented for all business processes related to the processing of electronic data in the event that the related information system becomes disrupted.

3.0 Roles and Responsibilities

The implementation of a security policy requires the participation of all users. The responsibility for control over access to information systems is a responsibility shared by the Department of Information Technology and the County divisions, departments, and offices.

Individual access control decisions should be assigned based on the job duties and responsibilities using the concept of "least privilege", which means that individuals are only given access and system rights necessary for completion of job tasks.

3.1 Security is Everyone's Responsibility

The following security responsibilities are shared by all:

- Participating in information security awareness program activities;
- Reporting security incidents;
- Complying with the County's Technology Security Policy, security guidelines, and any related procedures and responsibilities; and
- Protecting Anoka County electronic information assets from unauthorized access use distribution, disclosure, or destruction.

3.2 Users of Information Technology

Information users are the individuals, groups, or organizations authorized by Anoka County to access electronic information assets. Users have a responsibility to use electronic information assets only for the intended purpose. If the user has a question about the appropriate or the intended purpose of electronic information assets, the user must check with the appropriate system supervisor or manager for clarification.

Anoka County elected officials, appointed officials and employees shall not access private, confidential or not-public records or information unless their work assignments reasonably require access to such records. Unauthorized access may result in discipline up to and including termination as well as potential criminal sanctions.

3.3 Privileged User

A privileged user is a system administrator or other person with higher level system access who may be responsible for managing access to electronic information assets. Privileged users must only be given incremental access. Privileges will be granted to only properly qualified and trained County-authorized personnel. An increase in system access privileges must only be granted to the extent required by the job function of the privileged user, and as the level of trust with the privileged user increases.

3.4 Managers and Supervisors

Managers and supervisors are responsible for determining job functions and tasks as they relate to system access for electronic data and information assets. They must ensure that system access is not granted beyond what is necessary for the individual to perform their job duties. Managers and supervisors must also ensure that the Technology Security Policy, security guidelines, and any related processes and procedures are followed, including the completion of a Business Associate Agreement for HIPAA Compliance.

3.5 Data Owners

Data owners are individuals who have responsibility for the integrity, accurate reporting and use of electronic data. Administrative privileges for County information assets must only be granted to data owners where a business need is justified. Data owners are responsible for documenting and approving privileges. Segregation of duties must be employed to enhance the control over procedures where both the risk from, and consequential impact of, a related Information security incident would likely result in financial or other material damage to the County. Data owners need to periodically review access rights to determine the level and continued need of access rights for authorized users.

Data owners are responsible for ensuring that the appropriate data retention schedules for documents and records are being followed. Data owners must also take into consideration all County, State, Federal and any other pertinent rules or regulations related to their data in accordance with the Anoka County Personnel Rules and Regulations, the Anoka County HIPAA Policies and other applicable policies.

4.0 Department of Information Technology Role

The Department of Information Technology is responsible for maintaining County-wide technology and security standards and measures for the protection of electronic information assets including: policy development and documentation, virus and malicious software protection, firewalls, security assessments and audits, development of technology best practices and standards and coordinating the use of other security-related tools. In addition, the Department of Information Technology will provide consultation and leadership for security-related education, and the development of detailed processes and procedures within the framework of the Technology Security Policy.

The Department of Information Technology has several roles and responsibilities including:

- Facilitating and participating in all County Technology initiatives
- Ensuring that technology solutions meet security and best practice standards
- Enforceable security policies are documented and disseminated;
- Education and consultation is provided to County divisions, departments, and offices to facilitate security awareness;
- Reasonable security measures are taken and processes are in place to protect the County’s information assets;
- Ensuring that technology solutions are not duplicated; and that we take advantage of existing investments
- System resource usage is managed and monitored; and
- Security incidents are investigated, escalated, and remediated.

4.1 System Lifecycle

Information security is a continuous process and must be considered throughout the lifecycle of electronic information assets. Therefore, the acquisition, installation, implementation, asset inventory, maintenance, back-up and disposal of electronic information assets must be made within the framework of the Technology Security Policy, related guidelines, and in coordination with the Department of Information Technology.

4.2 Acquisitions and Disposals

Purchases/Acquisitions

All purchases of hardware and software must be made in consideration of the Technology Security Policy, Policy Supporting Documentation, county financial policies, and technical standards. County divisions, departments and offices must be familiar with related license agreements and ensure their compliance.

The Department of Information Technology will coordinate with the County Purchasing Office to determine hardware and software acquisition guidelines. Deviations or exceptions to the standards will be made based on business need and requirements. Product specifications must take into consideration business requirements, security, reliability, capacity, technical environment, ongoing maintenance, and recovery requirements. The Department of Information Technology will work with County divisions, departments, and offices to determine the best solutions for their requirements. Technology support, outsourcing or information hosting provided by outside vendors, contractors or other service providers must be coordinated with the Department of Information Technology. Technology services provided by outside vendors, contractors or other service providers must operate in accordance with the County's Standards and the Technology Security Policy and related guidelines.

Disposals

County divisions, departments, and offices must dispose all surplus electronic information assets once the asset is decommissioned. The following must be considered with the disposal of electronic information assets:

- Ensuring that all data is effectively removed;
- Ensuring that the disposal of physical information assets is coordinated with the County Purchasing Manager, who has the authority to dispose of surplus, scrap, excess, or obsolete County property and regulate its disposal in a manner, deemed to be in the County's best interest. The County's Purchasing Manager must ensure that the electronic information asset is cleared of any County information by a vendor that is DOD (Department of Defense) standard compliant.
- Ensuring that the disposal of data or electronic information complies with the Anoka County record retention policy, Minnesota statutes, and any Federal regulations.

4.3 System Implementation and Maintenance

The lifecycle of electronic information assets includes the implementation and maintenance of information systems with consideration given to developing change and version control processes, maintaining asset inventories, developing appropriate plans for system recovery, and developing plans for ongoing maintenance. Within this lifecycle, there is a need to ensure safe, secure, and reliable systems as well as maintaining the confidentiality, integrity, and availability of data. Systems developed by Anoka County must meet business requirements and specifications, be compliant with technical standards, this Policy, Minnesota and Federal laws, related guidelines, and be cost-effective and easy to maintain. Lifecycle management practices include the ongoing evaluation of systems for adherence to applicable laws, policies, guidelines, processes and procedures.

System Implementation

Implementation of information assets includes the use of software, databases, hardware and communication infrastructure, and must take into account the development of system recovery procedures, system documentation, the adoption of new manual procedures, and the processes for on-going system maintenance. Planning for the implementation of hardware and software must be coordinated with the Department of Information Technology. User practices and needs must be taken into consideration in the customization or development of software systems. All systems must be appropriately documented and tested prior to operational usage. Procedures and access controls must ensure compliance with applicable laws, policies, guidelines, processes and procedures, and provide for the confidentiality, integrity and availability of data.

Version control procedures must be used for system development and deployment. Adequate documentation must be maintained for historical reference, audit trail and change control.

All systems must be tested and accepted before being transferred to the production environment. Upgrades and updates to hardware and software must be properly tested by appropriately trained and authorized personnel before they are moved into the production environment.

Backup and Recovery

The Department of Information Technology will update and maintain a disaster recovery plan that reflects the recovery time objectives for data and applications as determined and prioritized by County leadership.

Information Technology will develop procedures to ensure that the backup of data meets the relevant recovery requirements based on the nature of the outage or disaster. The Department of Information Technology will maintain data backup guidelines that further define the process for the secure backup and storage of data files and software both onsite and offsite. The offsite storage facilities will be periodically reviewed to ensure proper security.

Any data maintained separately from the central county network must have a documented data backup and recovery procedure, which is the responsibility of the business unit Data Owners. The Department of Information Technology maintains an inventory of all county owned Servers, PCs, Laptops, and Tablets.

Inventories of other County electronic information assets including hardware and other electronic devices should be maintained by the County divisions, departments, and offices. County divisions, departments, and offices are responsible for updating and communicating changes in their hardware inventory to the Department of Information Technology.

Ongoing System Maintenance

Electronic information assets require ongoing upgrades and system maintenance, which must be coordinated with the Department of Information Technology. Periodic reviews of information systems should be performed to ensure that systems are adequately protected from undue risk. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability. Patches to resolve software bugs may only be applied where verified, tested by the appropriate parties, documented and authorized by the Department of Information Technology.

5.0 Data Security

It is important that Anoka County use safeguards to protect its electronic data assets from unauthorized release, use, or destruction. Safeguards can include, but are not limited to:
physical controls, user procedures, and hardware and software tools. Access to data must be carefully controlled, ensuring that only authorized personnel have access. Each County division, department, and office must ensure only authorized personnel are granted and retain access to electronic data.

5.1 Access Control

The responsibility for control over access to information assets is a shared responsibility of the Department of Information Technology and County divisions, departments, and offices. Individual access control decisions should be assigned based on the job duties and responsibilities necessary for the completion of job tasks.

User Accounts

Each user must be assigned a unique personal identifier or user I.D. User identification must be authenticated before the system grants access to electronic data. Authentication is the process of verifying the identity of a user who is logging onto a computer system or verifying the origin of a transmitted message.

Access decisions about user accounts must be documented by the data owner. Data owners are responsible for ensuring that verifiable authorization is in place for the creation and termination of accounts. Accounts must be disabled upon employee termination, contract completion, or a period of inactivity. Verifiable authorization includes ensuring that the user accessing the system has the appropriate role and responsibility, is a legitimate user, and is who they say they are.

Passwords

Passwords must be strong and well-guarded. Users are responsible for choosing secure passwords. Users must not divulge their passwords to others such as coworkers, or supervisors, or store passwords in an unsecured location. To account for lost or stolen passwords, data owners must institute procedures to verify the identity of the person requesting the reset of a password. For guidelines to creating passwords please visit the IT section of the County Intranet.

5.2 Storage Media and Transport of Data

Security must be considered when using electronic media for the storage and transport of data. Electronic media refers to any device or material that holds or transfers data in an electronic format, including the cloud. All users must consider the sensitive or non-public nature of the data, and the potential risk to the data when determining appropriate measures to safeguard storage or transport of electronic data. Any user that stores data on portable media must ensure the security of that data or media device and comply with required storage practices.

Required storage practices must be followed and include ensuring that:

- Private or confidential data is only transferred across networks or copied to other media when the confidentiality and integrity of the data can be assured through such techniques as encryption;
- Private or confidential data may not be saved to any unencrypted portable media;
- Retention policies and ease of access are considered when reviewing alternative storage media;
- Avoid leaving equipment in vehicles unless necessary, never leave unattended overnight;
- Portable hardware, devices and accessories must not be left in an unoccupied vehicle unless the vehicle is locked and the equipment is stored out of sight;
- When a user terminates their employment with the County, the supervisor is responsible for verifying that all portable hardware, devices and accessories are returned and the proper documentation is completed;
- The data is not stored on portable media unless the data is also available in a secondary location for future recovery and is protected from unauthorized access or theft; and
- A backup of the data is created, tested and is accessible.

5.3 Malicious Software

The Department of Information Technology will take steps to minimize the risk posed by malicious software. Malicious software may be introduced to the County network in a number of ways. All users of electronic data are responsible for recognizing and immediately reporting, suspected occurrences of malicious software and using reasonable precautions to prevent the introduction of malicious software. Precautions to prevent the introduction of malicious software should be taken when importing data onto computers through portable media or other electronic means such as through electronic mail, file transfers, or downloading from the internet. Prior to downloading any files or information from portable media to the County network, it is recommended that the Help Desk scans the files on the device for viruses.

5.4 Copyrights

It is the responsibility of County divisions, departments, and offices for assuring that commercial software is used only in accordance with licensing agreements, and that any proprietary software is properly licensed prior to installation on County equipment.

6.0 Proper Access To and Use of Electronic Information Assets

6.1 General Access and Use

Electronic Information Assets are available in many formats to Anoka County employees, officials of Anoka County, vendors, contractors and other personnel using county electronic information assets. In addition to the previously outlined procedures, the following guidelines govern access to and use of all electronic information assets provided to you by Anoka County.

For the purpose of this policy, Electronic Information Assets are defined as including:

- Hardware (which includes Servers, and Network Equipment Desktop PCs, Laptops, tablets, cellular and non-cellular telephones and any other fixed or portable technology that accesses or stores County information;
- Software;
- Third party provided tools, to include cloud-provided services or applications / “apps”;
- Personally-owned devices used to access or store County information;
- County owned data created, reviewed, saved or stored to any electronic system;
- Personal data created, reviewed, saved or stored to any County owned electronic system;
- Network connectivity and associated technologies to connect to the County network;
- The County’s Internet connection; and
- The County’s email system

Access to and use of electronic information assets is provided by the County for employee use. Department heads, division managers, and County officials will decide which of their employees or devices will be granted network and internet access. Nonexempt employees shall not access County technology assets outside of standard work hours, without prior permission.

It is each individual employee’s responsibility to ensure that any use of the network, County email internet access, and any other electronic information asset is in accordance with this Policy and any other County policies.

Employees must proceed in their access to and use of electronic information assets regardless of the medium used, with the expectation that the access may be reviewed by any authorized representative of the County for any purpose related to County business. The County, in its discretion, may use computer programs that monitor activities related to use of County technology, checking for particular words, actions or patterns of activity, or for purposes of assuring system security and compliance with County policies.

Electronic asset usage by an employee may be reviewed to determine whether there have been any breaches of security, or violations of County policy on the part of the employee. Electronic communications may be reviewed by the appropriate supervisor or other county officials in accordance with the process outlined by the County Attorney’s Office.

All County assets and information are County property and are subject to the requirements and restrictions of all applicable State and Federal Statutes and Regulations concerning the collection, creation, storage, maintenance, dissemination and access to information created and/or maintained by the County including, but not limited to, the Minnesota Government Data Practices Act. The County reserves the right to access and disclose all information created, accessed saved or distributed for any purpose not specifically prohibited by Statute or Regulation.

All devices, whether County issued or personally owned, used to access County information and conduct County business are subject to discovery pursuant to the Minnesota Government Data Practices Act or such other applicable State or Federal Statute or Regulation.

It is the intention of the County in the use of the County's Electronic Mail System that such data and information contained in or attached to such messages is not an official transaction of the County. The County's Electronic Mail System is meant to be a temporary medium for the transmission of data. All records required to be maintained pursuant to any applicable Statute or Regulation shall be maintained separate from the County's Electronic Mail System.

6.2 Allowed communication with third parties (Non-County Employees)

6.2.1 The County Electronic Mail System is open to all state agencies, political subdivisions, and the public to provide a means by which members of state agencies, political subdivisions, and the public may communicate with the County.

6.2.2 Messages sent between the County and members of state agencies, political subdivisions, and the public may be used by the County for any Government or Business purpose.

6.2.3 Members of state agencies, political subdivisions, and the public who subscribe to the County's electronic mail system will be informed of applicable rules and will be required to agree to County policies with respect to access and disclosure of electronic mail messages.

6.2.4 Always use care in addressing messages to ensure messages are not inadvertently sent to Non-County Employees that are meant only for County Employees.

6.3 Electronic Information Assets may not be used for "snooping"

6.3.1 It is a violation of County policy for any employee or County official to use the electronic mail or other Information Assets for purposes of satisfying idle curiosity about the affairs of others, with no work-related purpose for obtaining access to the files or communications of others.

6.4 Monitoring for Security Violations

6.4.1 The County reserves and intends to exercise the right to access the contents of electronic mail communications for any business purpose.

6.4.2 The electronic mail system is provided by the County for your use as an employee. You should treat it like your shared filing systems - with the expectation that messages sent on County business or with the use of County facilities will be available for review by any authorized representative of the County for any purpose related to County business at any time.

6.4.3 Electronic mail communications of an employee may be utilized to determine whether there have been any breaches of security, violations of County policy, or other violation of duty on the part of employees. Electronic communications may be reviewed by the appropriate supervisor or other county officials in accordance with the process outlined by the County Attorney's Office.

6.4.4 The County, in its discretion, may use computer programs that monitor electronic mail messages electronically, checking for particular words or patterns of activity, for purposes of assuring system security and compliance with County policies.

6.5 Limitations On Disclosure And Use Of Information Obtained By Means Of Access Or Monitoring

6.5.1 The contents of electronic mail sent by, between, and/or to County Employees may be disclosed within or outside the County without the permission of the employee at any time for any purpose deemed necessary by the County subject to any limitations imposed by any applicable State and Federal Statutes and Regulations concerning the collection, creation, storage, maintenance, dissemination and access to data created and/or maintained by the County, including but not limited to the Minnesota Government Data Practices Act.

6.6 Publishing on The Internet

6.6.1 Anoka County recognizes the value and potential of publishing on the Internet. Departments must work with the County's Public Information Department to determine how their presence on the Web site will be developed to promote cohesiveness and prevent duplication of effort.

6.6.2 Contents of all electronic pages must be consistent with Anoka County's policies and procedures and local, state, and federal laws. Electronic publications are subject to the same County policies and standards as print publications. Departments may work with the County's Web Site Coordinator to create electronic home pages or publication pages that are intended for official Anoka County business.

6.6.3 Web pages on the official Web site of Anoka County may contain links to pages on Web sites that are not controlled by or under the authority of Anoka County Government. Departments should work through the Public Information Department to communicate recommendations relating to links to non-County websites.

6.7 Personal Use of County Electronic Information Assets

While incidental and occasional personal use of the County's electronic information assets is permitted, such use will be treated no differently than accessing County electronic information assets for business purposes. Anoka County is not responsible for any personal information created, accessed, saved or distributed when using County electronic information assets for personal purposes and the employee acknowledges that any such information is subject to discovery pursuant to the Minnesota Government Data Practices Act or such other applicable State or Federal Statute or Regulation. Incidental and personal use of County electronic information assets is subject to all limitations specified in this policy, the County Anoka County Personnel Rules and Regulations, and complies with the following:

- Does not interfere with County business usage;
- Does not interfere with employee's job activities;
- Does not interfere with another employee's job activities;
- Does not transmit or receive any material in violation of any Federal or State laws or regulations;
- Does not result in an additional or unapproved expense for the County; and
- Does not contain or infer threatening or inappropriate content for the County work environment, including, but not limited to, intimidating, sexually oriented, obscene, offensive, or abusive material and/or language.

6.7.1 Prohibitions on the Use of County Electronic Information Assets. It is a violation of this policy for any County official or employee to:

- Use the County's technology resources for purposes of satisfying idle curiosity about the affairs of others, with no work-related purpose for obtaining access to the files or communications of others.
- Access, distribute or create any material that is a violation of the Anoka County Personnel Rules and Regulations.
- Intentional or malicious actions which would interfere with the operation of the County network or the work of others on the network. This would include, but is not necessarily limited to, excessive downloading of programs or data, or adversely affecting available bandwidth or other network resources, including storage space.
- Misrepresent their identity or affiliation in any communications.
- Send harassing, intimidating, abusive or offensive material to or about others.
- Intentionally intercepting, disrupting or altering electronic communications packets (without necessary authorization).
- Using another employee's identity and password. The sharing of credentials should be limited to County employees that must share a workstation with other County employees.
- Accessing private data for which there is no business or job-related need to do so.

7.0 Wireless Devices

Wireless devices are one means used to access County technology. All the rules and regulations outlined in the Technology Security Policy apply to the use of wireless devices. Additional regulations relating to wireless devices are outlined in this section.

7.1 Information Technology Requirements

- The Anoka County Board authorizes the Director of Information Technology to review and authorize a list of acceptable Operating Systems and other wireless technology security requirements to ensure the County complies with security and privacy requirements pursuant to Minnesota and Federal law, and County requirements as follows:

- A County-owned wireless device must utilize an Operating System and other security requirements approved by the Director of Information Technology.
- Any personal device used to access County information must utilize an Operating System and other security requirements approved by the Director of Information Technology.
- Information Technology is responsible for activating e-mail access on wireless devices and supporting the ability to access County e-mail and County business features, (e.g., contacts, calendar, tasks from the County e-mail system).

The Employee is responsible for the support of wireless device features and accessories such as 3rd party apps, media, contacts, device preferences, and other non-County business features.

The Operating System requirements and other security requirements change as technology evolves. For a list of current requirements, please reference the Technology Security Policy Supporting Documentation.

7.2 County Financial Policies

Plan costs and costs reimbursement (if applicable) are detailed in the County's Financial Policies.

7.3 Personally Owned Wireless Devices

The Division Manager Department, Head or authorized Supervisor may:

Authorize staff to use their personal wireless device for County business, if the device meets the Operating System and any other security requirements recommended by the Director of Information Technology. All County employees using wireless devices for County business must comply with all applicable Federal, State and Local laws and County policies.

Division Managers, Department Heads or authorized designee is responsible for:

- Ensuring that staff is educated on procedures to securely access County information on a wireless device;
- Authorizing staff to use personal wireless devices for County business, if the wireless device meets the requirements recommended by the Director of Information Technology; and
- Keep wireless device records on file as required by the business units Records Retention guidelines.

Any employee who would like to connect their personal wireless device to the County e-mail system must obtain approval from their Division Manager or Department Head and agree to the terms of the policy.

7.4 Remote Access

Remote access must be controlled, secured and approved by the Department of Information Technology. Remote access to the County's network and computer systems will only be permitted:

- Through approved devices;
- By authorized users that are authenticated;
- Where the data is encrypted, and

- Where privileges are restricted.

All dial-up access points will be managed and maintained by the Department of Information Technology. The unauthorized installation or use of devices to support dial-in access, wireless devices, or other non-county approved devices is prohibited.

County technology standards, policies, guidelines and procedures must be followed for any access through remote devices. Each County division, department, or office must establish procedures to ensure that remote workstations and mobile devices are utilized according to the County-wide Security Policy, and guidelines.

Remote access for third party administration of County computer systems, or County network devices must be approved by the Department of Information Technology. Third party access will require a signed Anoka County Technology Usage Agreement (see Supporting Information) by each person that requires access.

7.5 County Owned Wireless Devices

Purchasing is responsible for:

- Maintaining an inventory of all county owned wireless devices. This inventory will be provided to the Department of Information Technology as needed for security purposes.
- Conducting an analysis of the wireless devices and plans as necessary to ensure that the County is utilizing the best value wireless service providers, in conjunction with the security requirements of the device as determined by the Department of Information Technology.
- If activating phone or data service (applies to County owned devices), activate service with service provider and notify Information Technology to have email service enabled.
- Work with County units to acquire wireless devices in accordance with County Purchasing Policies.

For information on backing up data from a wireless device to the cloud, please see section 9.0.

8.0 Data Communication and Network Security

Physical and electronic access to the County's data communication and network, including related hardware, software and cabling, must be secure and well protected. Data communication and network security is related to the following infrastructure:

- The County's local and wide-area communication network;
- The County's internal wireless network;
- Cloud-based computing and Application Service Providers (ASPs)
- Cloud-based storage
- Software as a Service (SaaS) Providers
- Virtual Private Networks (VPN's); and
- Any other County data communication system.

8.1 Access to the County's Network

Access to the County's network and devices is controlled by the Department of Information Technology and only granted to trained and qualified personnel with careful consideration of potential risks, security issues, and applicable statutes and rules. Password policies for accessing network devices such as switches, routers, and firewalls is restricted based on the concept of least privilege and with appropriate consideration of security issues. Passwords must be complex, kept confidential and not shared with others. Passwords for network devices must be changed periodically, and access must not be left active after an employee termination, contract termination, or if access is no longer required for completion of job tasks.

All devices, whether County issued or personally owned, used to access County information and conduct County business are subject to discovery pursuant to the Minnesota Government Data Practices Act or such other applicable State or Federal Statute or Regulation.

8.2 Network Firewall

Network Firewalls must be configured to support the following minimum requirements:

- County network access will be limited to allow for only legitimate or established connections. An established connection is defined as a connection that receives traffic in response to a request submitted from within the County's secure network.
- Any exception required of the firewall for inbound traffic to the County's network, such as access from a workstation outside the County network or access through a Virtual Private Network (VPN), must be approved by the Department of Information Technology.
- Access through console and other management ports must be appropriately secured or disabled.
- Failed access attempts must be logged and the logs must be periodically reviewed.
- All firewall hardware must be located in a physically secure environment.

9.0 Cloud Computing, Applications and Services

As the County continues to pursue options for secure, cloud-based computing, applications and services, opportunities will arise to conduct more business "in the cloud" through Application Services Providers (ASPs), or via Software as a Service (SaaS).

As with any other technology solution, Divisions, Departments and Offices considering these newer means of processing or storing information and data must work with Information Technology to determine if the solution meets the data privacy, technical and security standards of the County. Extra consideration will be made if the potential solution will store or process unencrypted, sensitive, private or HIPAA related data.

9.1 Network Design

The County network must be designed and configured to provide controlled access to County computer systems while preventing unauthorized access, administrator abuse, and general physical and logical harm. The Department of Information Technology must use best practices in configuring and managing the County's network to minimize downtime, create redundancy, maintain integrity, provide maximum performance and enhance security.

Documentation related to physical and logical network diagrams, network devices, access lists and other network configurations must be kept up-to-date and readily available to the authorized staff supporting or maintaining systems. The documentation must be reviewed and updated annually. All critical equipment owned, leased or licensed by the County must be supported by appropriate maintenance vendors with qualified, trained and certified engineers.

9.2 Encryption

Encryption or other security techniques must be used for Private or Confidential data that will be stored in a non-secure location or transmitted outside of the County network (such as over the internet). The Department of Information Technology will coordinate and approve all encryption products and other security techniques.

One security technique used to minimize the risk of information loss or exposure is two-factor authentication. Using this technique, each user has something they “own” and something they “know” to validate access to Private or Confidential data. Something they “know” is their user name and password. To provide for additional security, in case a password is stolen, users that access the network remotely are also required to utilize something they “own”, referred to as a security token or FOB.

The distribution of security tokens must only be made through appropriate, secure and approved methods. Assignment and management of tokens is restricted to authorized and trained personnel in the Department of Information Technology.

9.3 Cabling

Network cabling must only be installed and maintained by authorized, trained, and certified cabling personnel and vendors, approved through the Department of Information Technology. All network cabling must be installed to the County’s current cabling technology standard.

To ensure the integrity of the County’s network, access through physical wall jacks must be controlled, secured and approved by the Department of Information Technology. Any unused network wall jacks should be disabled. The Department of Information Technology can be contacted if an active network jack needs to be disabled.

10.0 Supporting Documentation

As noted on page four, in support of this policy is a document titled “Anoka County Supporting Documents and Information” containing:

Appendix A - Glossary of Technology Terms

Appendix B - Password Guidelines

Appendix C - Incident Reporting

Appendix D - Technology Usage Agreement

Appendix E - Business Associate Agreement

The Supporting Documentation may be updated on a routine basis as technology, security, or County business standards evolve.