Anoka County
COUNTY ADMINISTRATION
Information Technology

Anoka County

Technology Security Policy

Appendix A

Glossary of Technology Terms

TECHNOLOGY SECURITY POLICY SUPPORTING DOCUMENTS

Appendix A - Glossary of Technology Terms

Application Service Provider	Application Service Provider - An application service provider (ASP) is a company that offers individuals or enterprises access over the Internet to applications and related services that would otherwise have to be located in their own personal or enterprise computers.
Authentication	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.
Auto Forwarding	Auto Forwarding is the process of automatically forwarding e-mail messages to one or more users when certain conditions (or rules) are met.
Auto Response	Auto Response is the process of automatically sending a reply to the sender of an e-mail message based on rules or configurations that are set in the e-mail system. For example, if you need to be out of the office for several days, a rule could be configured to automatically send a reply to incoming messages advising others when you'll be returning to the office.
Availability	Availability is an important concept with regard to security and means that access to an electronic information asset, such as data or an information system, is not denied to authorized users.
Backup	Backup is the process of transferring software and data to alternative media, such as tape, to be used to recover systems in the event of system malfunction or disaster.
Business Logic	Business Logic or business rules are used in computer applications to ensure the software operates according to the business requirements for processing transactions and information.
Cloud Computing	Cloud Computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is often referred to as an activity that takes place "in the cloud". It enables on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released. Cloud computing and storage solutions can provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party data centers.
Cloud Storage	Cloud storage is a model of data storage in which the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running.
Confidentiality	Confidentiality is an important concept with regard to security and means that information deemed sensitive or not-public is protected to make it unavailable to those who do not have the necessary approvals to access it.
Contractor	See Vendor.
Critical Application	A Critical Application is one that is so important that its malfunction, loss, or unavailability would have a significant impact on the continued operation of the County.
Data Owner	Data owners are individuals who have responsibility for the integrity, accurate reporting and use of electronic data.
Disaster Recovery Plan	A Disaster Recovery Plan documents steps that must be taken to recover electronic systems and processes in the event of a system malfunction or a disaster.

TECHNOLOGY SECURITY POLICY SUPPORTING DOCUMENTS

Disposals	Disposals refer to the removal of obsolete information assets when there is no further use for them in the County.
Electronic Information Assets	An Electronic Information Asset includes hardware, software, and electronic data systems including such items as: computer hardware and devices, mobile devices, network and telecommunications, Internet based communication, software applications and related services, data and databases, information technology facilities, and off-site data storage.
Employee	For purposes of this policy, an employee is defined as all persons employed by Anoka County whose pay comes in whole or in part from County funds and/or is working under the direction or control of any County official, division, department, or office. The term "employee" shall include those who work for Anoka County on a voluntary basis with or without pay or other form of compensation. The term "employee" shall also include any person serving with or without compensation in any form as a member of a board, task force or commission established by Anoka County.
Encryption	Encryption is a technique used to protect data by transforming the data from the original format to a difficult to interpret format.
Financial Policies	The Financial Polices is approved by the County Board to set forth the basic framework for the overall fiscal management of Anoka County. The County Financial Policies can be found on the County's Intranet web site.
Firewall	A Firewall is a method, device, or software that is used to implement security policies designed to keep a network secure from intruders.
Guideline	Guidelines are used to further provide detailed documentation of functions in support of this County-wide Technology Security Policy document.
Hardware Fault	A Hardware Fault is an error or other malfunction on a piece of hardware or a computerized system.
Help Desk	The Help Desk is a work unit in the Department of Information Technology that takes the first call for help for all County computer problems. Users may contact the Help Desk.
HIPAA	HIPAA is the federal Health Insurance Portability and Accountability Act that sets a national standard for protecting the privacy and security of medical information.
Information Asset	An Information Asset includes hardware, software, and electronic data systems including such items as: computer hardware and devices (including thumb drives, phones, tablets, CDs, DVDs, external hard drives and other portable media) network communications, software applications and related services, data and databases, information technology facilities, and off-site data storage.
Integrity	Integrity is an important concept with regard to security and means that the electronic information asset is correct and has not been altered or corrupted in some way during transmission, processing, or while in secure storage. It also means that programs, applications, procedures, and systems function as intended.
Least Privilege	The concept of least privilege means that individuals have access and system rights necessary for completion of job tasks, and no more.
Malicious Software	Malicious software is software designed to destroy, aggravate and otherwise interfere with the operation of the County's electronic data systems. Examples include, but are not limited to: viruses, worms, spyware, logic bombs, macro viruses, and Trojan horses.
Not-Public Information	Any information classified by statute, federal law including HIPAA regulations, or temporary classification as confidential, private, nonpublic, protected nonpublic, or protected health information, which must be protected from unlawful disclosure.

TECHNOLOGY SECURITY POLICY SUPPORTING DOCUMENTS

Offsite Storage Facilities	Offsite Storage Facilities are located a distance from the primary County buildings, and are used to store backup and other required items that will be used in the event of system malfunction or a disaster for the recovery of systems.
Operating System	An operating system (also known as an OS) is a collection of software that manages computer hardware resources and provides common services for computer programs. The operating system is a vital component of the system software in a computer system.
Password	A Password is a secret series of characters that enables a user to access an information asset such as a computer, or application software.
Physical Security	Physical security is the protection of computer hardware and devices from physical risks that could cause serious loss or damage.
Portable Media	Portable media refers to devices that easily transported and includes such items as removable drives, disks, laptops, and personal data assistants (see information assets)
Privileged User	A Privileged User is a system administrator or other person with higher level system access who is responsible for managing access to electronic information assets.
Procedure	A Procedure is administrative, detailed instructions used to document a process related to policy or guidelines.
Purchasing Policy	The County Purchasing Policy provides a framework to govern the purchasing process in the County, and can be found in the County Financial Policies on the County's intranet website.
Remote Access	Remotes access is any access to the County's systems from outside the County's physical network.
Recovery Time Objective	The recovery time objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. It can include the time for trying to fix the problem without a recovery, the recovery itself, testing, and the communication to the users. Decision time for user's representative is not included.
Safeguards	Safeguards are used to protect information assets from unauthorized release, use, or destruction. Safeguards can include physical controls, user procedures or hardware and software tools.
Security Audit or Assessment	A Security Audit or Assessment is a review of security policies, guidelines, procedure, and safeguards measured against industry best practices to determine improvements that could be implemented to improve security.
Security Patch	A Security Patch is a fix to a computer program, delivered as a piece of programming code that is applied to an application to fix an existing problem or prevent a problem from occurring.
Segregation of Duties	Segregation of duties means that job tasks are specifically assigned to separate individuals to enhance control over procedures where both the risk from, and the consequential impact of, a related information security incident would likely result in financial or other material damage to the County.
Software as a Service (SaaS) Providers	Software as a service is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software". SaaS is typically accessed by users using a thin client via a web browser.
System Administrator	A System Administrator is an individual that has the job task of performing a high-level function related to a computer application or system.

TECHNOLOGY SECURITY POLICY SUPPORTING DOCUMENTS

System Lifecycle	A System Lifecycle is the process that information assets go through from their acquisition to the termination of their use and subsequent salvage.
System Recovery Procedures	System Recovery Procedures are the documentation of steps that need to be taken to recover a computer system or function in the event of a malfunction or disaster.
Technical Standards	Technical Standards are used to establish uniformity in common technology infrastructures, applications, processes or data.
User	Users are the individuals, groups, or organizations authorized by the County to access information assets.
User ID	A User ID is an identifying symbol or set of characters assigned to a specific information user.
Vendor	A Vendor is an individual, group or organization that is working under the authorization and direction of a County division, department, or office to complete a task or function that uses or affects a County electronic information asset.
Virtual Private Network	A Virtual Private Network (VPN) is software or hardware that is used to provide additional security for accessing systems across the public networks, such as the internet.
Version Control Procedures	Version Control Procedures are documented processes used to maintain updates to software, and to control the version used for system processing.
Virus	See Malicious Software.
Wireless Network	Wireless Network, for purposes of this policy, means the implementation of access points to allow laptops to connect to the County's network infrastructure, without a physical wired connection.