City of Appleton Policy	TITLE: Network Security and Use of Technology	
ISSUE DATE: March 2011	LAST UPDATE: August 2017	SECTION: Miscellaneous
POLICY SOURCE: Information Technology Department	POLICY AUDIENCE: All City of Appleton Employees	TOTAL PAGES: 9
Reviewed by Attorney's Office Date: December 2010	Committee Approval Date: March 23, 2011	Council Approval Date: April 6, 2011

PURPOSE

Computer information systems and networks are an integral part of business at the City of Appleton. The City has made a substantial investment by providing computer systems to each department to improve the quality and timeliness of its services. The following policies have been established to:

- Protect this investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the reputation of the City of Appleton.

POLICY

All City of Appleton technology resources, including but not limited to, computers, printers, copy machines, telephones, internet access, email, voice mail, wireless connections, smart devices and remote network access, are provided solely for business purposes. At any time and without prior notice, the City of Appleton maintains the right and ability to examine any systems, inspect, and review all data stored in these systems. Any information, whether contained on a hard drive, removable media or in any other manner may be subject to scrutiny by the City. Failure to comply with this policy can potentially lead to disciplinary action up to and including dismissal. In order to ensure compliance with this policy, the City has employed methods to monitor the use of systems and devices as well as use of the internet and content of email. The City specifically reserves the right for authorized personnel to access, retrieve, read and/or remove any communication that is created on, received through, or sent via the email system, to assure compliance with all City policies. The City reserves the right to filter or remove any non-City related files from email or electronic storage including but not limited to specific file types, such as WAV, AVI, MP3, MP4, and MPG files, that are not business related. Other executable files such as EXE, BAT, CMD, DOCM files may also be filtered, as this is a primary method of transporting malware. Email filtering can also be used to detect certain phrases that may also be prevented from incoming and outgoing messages. Such monitoring will be used for legitimate purposes only, and are accessed in the following manners:

- A request to the Human Resources and the Information Technology Director and approved by the Department Head.
- By authorized staff within the Information Technology Department to troubleshoot the network or supported systems.
- By the Information Technology Department for trend analysis and reporting to ensure that, systems in place are effective in protecting the assets of the City.

For purposes of Library administered systems and networks, Library Administration and Network Services serve the review and approval functions of Human Resources and Information Technology as listed. Other sections of this policy relating to hardware and software apply only to the City networked "administrative" computers located at the Library and not to the public access systems. ~~Library rules and procedures are subject to review and approval by Human Resources, Information Technology and the City Attorney.~~ The Library Board shall have the powers and duties set forth in Wisconsin Statutes Sec. 43.58 and, whenever practicable, shall exercise those powers and duties in accordance with this and other City of Appleton ~~personnel~~ policies. No City of Appleton policies shall be interpreted in a way that usurps the Library Board's powers and duties set forth in sec. 43.58, stats.

DISCUSSION

The Information Technology Director is responsible for the implementation, development and on-going support of computer and technology related systems in the City to ensure their availability, security, reliability and cost effectiveness in increasing effectiveness of administrative, operational and communication requirements for all City staff. This policy is intended to implement standards and requirements that will assist with that responsibility. The Information Technology Director will review this policy periodically and make any recommendations for changes to the Common Council for approval.

DEFINITIONS

A. Department Head: refers to the Director or Manager of a department or agency, or the department's designee.
B. Internet: refers to an "External" network with many web servers containing web pages used to display information to the public. City of Appleton's Internet URLs include www.appleton.org , my.appleton.org , www.myvalleytransit.com , www.appletonparkandrec.org and gis.appleton.org.
C. Intranet: refers to the "Internal" City web pages used to display information that is only accessible and only pertains to City of Appleton employees and departments via the Local area Network (LAN) http://intranet.
D. Smart Device: cell phones, iPad, tablet, Microsoft Surface etc.
E. Filtering: to filter and block certain items from the Internet based on URL address, category, user, port, protocol, attachments and other criteria.
F. Malicious Code: Computer viruses or other programs introduced purposely to disrupt, destroy or damage City information technology.
G. Spam: Unsolicited email received to promote a product.
H. Network: refers to the system of interconnected computer and technology devices and the means through which they are connected. This includes but is not limited to servers (including the iSeries), switches, routers, modems, computers, laptops, printers, copy machines, telephones, smart devices, wireless access points as well as any means of connection between them or to the Internet.

RESPONSIBILITIES

A. Information Technology Director Responsibilities
    - Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policies.
    - Provide appropriate support and guidance to assist employees to fulfill their responsibilities outlined in the policies contained in this document.

- Maintain and update this policy periodically.

B. Director/Manager Responsibilities
    - Ensure that all personnel are familiar with and comply with this policy.
    - Create performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe the policies contained in this document.

C. User Responsibilities
    - Contact Information Technology for any hardware repair and software installation, as they are the responsibility of the Information Technology Department.
    - Keep the display, keyboard, and other equipment clean.
    - Any work done on your computer is considered work done for hire and as such is the property of the City of Appleton.
    - The protection of confidential information is vital to the interests and success of the City. Employees are prohibited from disclosing confidential information to any unauthorized person or entity.
    - Do not attach CD's, DVD's, USB Jump Drives and other portable media of unknown origin to City computers or systems.
    - Any employee who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the Information Technology Helpdesk at 5893.

PROCEDURES

A. Physical Security
    - Hardware (computers, printers, telephones, copiers, smart devices etc.) cannot be purchased, installed, configured or relocated without prior approval from Information Technology.
    - Outside or personal computer equipment cannot be connected to the City of Appleton Network in any way unless approved by the Information Technology Department.
    - Modems are not permitted on any computer unless approved by Information Technology, who will inventory all active modems.
    - All users are prohibited from removing or disabling any administrative, security, or virus scanning software from their computer.
    - Software programs downloaded from the internet or those brought to work by a user cannot be installed on any computer without prior Information Technology approval.
    - Computer monitors that will display PHI (Personal Health Information) should not be viewable from outside the employees' office or workstation. Each PC should be locked into screensaver mode or logged off before a worker leaves their office. In addition, screen savers can be set to automatically take effect after 20 minutes of inactivity at the Information Technology Departments discretion.

B. Password Security

    - All user passwords are required to be changed every 90 days. Users will be prompted to change their passwords.

- Information Technology will configure systems to require passwords containing requirements that increase password strength whenever possible.
- Passwords must not be accessible to any other users. Each user is solely responsible for all computer transactions, such as internet use and file access, completed using his or her network and application login name and password.
- Information Technology may ask a user for his or her password to install and troubleshoot hardware and software. Information Technology will maintain the confidentiality of the password or, if requested, can reset the password for the user to change at next logon. Information Technology may also reset the password to troubleshoot a PC. If this is the case, Information Technology will prompt the user to change the password at next logon. Users can also change their own network password at any time by pressing Ctrl+Alt+Del and clicking on the "Change Password" button.
- Contact the IT helpdesk at #5893 if a password is forgotten. Information Technology can only reset passwords if needed, if you signed up for password recovery, you may be able to reset your own password.
- Network, Internet, Remote Access and Email access are associated with the user's logon and password. If the user is not granted permission by the department to use these resources, their profiles will restrict them from doing so.
- Each department should request network access for their external users that may need to access their computer systems such as contractors, via an Information Technology request. Users are prohibited from sharing their passwords with other users, contractors or outside personnel.

C. File Security

- Based on the information from the work requests, Information Technology assigns folder and file permissions to specific users and groups of all directories (PC Network) and libraries (iSeries) to control access to data on the network.
- All data files in the network are required to be stored on network drives as assigned and available to each user. The local drives (commonly known as "C" drives) of individual computers are not backed up and any data stored in that manner is vulnerable to unauthorized access and data loss. Any data stored on local PCs will be the sole responsibility of the end user.

- If a document is highly confidential or sensitive in nature, you should store it in a private directory.
- The Information Technology Department will make every effort to prevent viruses from infiltrating City computer systems. Each PC must have a virus scanner installed and configured. In addition, a network based virus scanner for all incoming and outgoing messages will be maintained to assist Information Technology in stopping viruses from spreading.
- All Information Technology employees who may have, or may gain access to sensitive data or law enforcement records or systems must undergo a complete background check, including fingerprinting through the Appleton Police Department prior to obtaining this access. Those who may access information maintained by CIB must also meet all requirements as designated by CJIS to include completion of the Security Awareness training module through the

TRAIN applications.

D. Employees (New & Departing)
    - New & Transferred Employees—Each Department is requested to notify the Information Technology Department at least 2 weeks in advance whenever possible, of the need for new or changed network or iSeries access.
    - Before any Network, iSeries or Internet related access is granted; an Information Technology request must be completed and authorized by the employee's department head. The Information Technology work request should define permitted computer program and data access.
    - Departing Employees—Each Department is required to give the Information Technology Department advance notice of employees departing employment at City of Appleton whenever possible. An Information Technology work request must be completed and should define when the user profiles should be disabled and/or deleted and how the user's data files and old emails should be handled.

E. Network Drives
    - When users logon to the network, Information Technology scripts each user's drive mappings.
    - Each department has a J drive to allow the sharing of data files within the department only. Only members of each department can access the department folders under J:\ unless the Department Head requests in writing to allow another user access.
    - H:\(HOME)= The H:\ drive is for personal files that only the authorized user and the Information Technology Department has access to.
    - Information Technology may also map other drives for departmental specific purposes.

F. Remote Network Access
    - The City of Appleton Information Technology Department can provide remote access to the City network to allow employees the ability to perform work from remote locations. It is the responsibility of the City of Appleton employees, contractors, vendors and agents with remote access privileges to the City of Appleton's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the City of Appleton. An authorization form needs to be completed and signed by the employee and Department Head before remote access will be permitted. This document should outline when the employee is permitted to utilize this service.

G. Wireless Network Access
    - Smart devices belonging to employees that are for personal use only, are not allowed to connect to the network by a network cable plugged into a data outlet or Network Wireless, but only allowed to connect to the Guest Wireless.
    - Employees may use their personal mobile device to access the following company-owned resources: email, calendars, websites and contacts.
    - Connectivity and device operation issues are not supported by technical staff members; users should contact the device manufacturer or their carrier for operating system, network, or hardware-related issues
    - The Information Technology Department reserves the right to disconnect devices or disable services without notification.
    - The employee assumes full liability for risks including, but not limited to, the

partial or complete loss of City and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

- City of Appleton reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined. This policy is intended to protect the security and integrity of City of Appleton's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

H. Training

- Information Technology will coordinate or provide training to users on features of software owned by the City when requested. When requested, Information Technology will assist with recommending a contracting company to train a group of users regarding the use of a specific software program.
- Department Heads may request to have their department trained on the use of any City supported software program or feature.

I. Remote Control

- PC Remote Control software is used to manage and troubleshoot computers remotely over the network without Information Technology having to physically go to the site of the computer. This functionality is password protected and only authorized Information Technology staff has the password to access each PC in this manner. Before Information Technology takes control of any PC using the remote control software, when applicable they will normally notify the user using one of the following methods in order of precedence:
- Calling the user directly.
- Contacting a clerical employee of the department.
- Calling a nearby employee to alert his or her co-worker.
- If the user is, unavailable Information Technology may need to remote the machine anyway to remedy an issue.

J. Software/Hardware Policy

- Software, hardware, and network systems are intended to be used for business purposes only to increase the quality and timeliness of services provided by the City.
- All software acquired for or on behalf of City of Appleton or developed by City of Appleton employees or contract personnel on behalf of the City is and shall be deemed City property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements**.**
- As required by the City's Procurement Policy, all purchasing of City of Appleton software shall be centralized with the Information Technology department to ensure that all applications conform to City software standards, are purchased at the best possible price, and inventoried. The department head must approve all requests for City software. The request must then be sent to the Information Technology Department for approval and to determine the standard hardware or software that best accommodates the desired request.
- Unless otherwise provided in the applicable license, notice contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be in violation of federal and state law. In addition to violating such laws, unauthorized duplication of software is a violation of this Software/Hardware Policy. Employees may purchase software for their home PC's under the City's

Microsoft Home Use Program. Purchases made under this program are between Microsoft and the user. The City of Appleton will not support installation or maintenance of this software on employee's personal home devices.

- Numerous software titles are installed and supported by Information Technology on an as-needed basis. All software utilized on City equipment must be authorized by the Information Technology Department.
- Employees needing software other than those programs available to them must request such software from the Information Technology Department. Each request will be considered on a case-by-case basis in conjunction with the software-purchasing section of this policy.

K. Hardware

- Hardware is defined as all computer, printer, smart devices, copier or network technology equipment that is part of, attaches to, or integrates with any portion of the City network both wired and wireless. All hardware equipment acquired is purchased using standards developed by the Information Technology Department. All such hardware must be used in compliance with applicable licenses, notices, contracts, and agreements.
- All purchasing of City computer hardware equipment shall be requested through the Information Technology Department to ensure that all equipment conforms to City hardware standards and is purchased at the best possible price.

L. Computer Hardware & Software Disposal

- Information Technology will make the final determination of when and how to dispose of old computer equipment. Information Technology will then prepare all old computer equipment for disposal by destroying all hard drives to remove direct access to any information they may contain through certified technology recycling vendors. The City hardware inventory will be updated and all old computer equipment will be traded in when purchasing replacement equipment or disposed of in an environmentally sound manner. The Information Technology Department reserves the right to sell select computer equipment through approved processes. The Information Technology Director must approve exceptions to this policy.

M. Copy Machines

- Copy machine negotiations and contracts are also maintained by the Information Technology Department with assistance from the Purchasing Manager. An effort to network copy machines will be made to reduce the number of stand-alone printers, scanners and fax machines the City needs to purchase. The Information Technology Director will approve new copier leases based on a survey of each department's need and ongoing equipment and service costs. Any copy machines that are returned to vendors at end of lease will surrender the hard drive to the IT Department to be destroyed in the same fashion as the computer hard drives are. In the event a unit is disposed of in another manner, the hard drive will be removed and destroyed by Information Technology before disposal.
- All employees should use due diligence to ensure any printed information or documents that may contain sensitive data are not left in open view or unsecured file systems. Once these documents are no longer needed, employees should ensure they are either be shredded or placed in secure document disposal bins provided by the City.

N. Desk Telephones

- The Information Technology Department shall be responsible for the administration of non-cellular based telephone use, including the acquisition of desk telephones, non-cellular wireless telephones, specific contracts and service plans for telecommunications, and the maintenance of systems that provide tracking and recording capabilities for calls placed or received on City telephone systems.
- To ensure accuracy of the City's Enhanced 911 service, Information Technology must be informed before any office phone is moved to an alternate location.
- Departments can be provided a monthly itemization for all long distance and local telephone calls placed by employees of their respective departments.
- All employees assigned a dedicated telephone number will be provided with a personal voice mailbox number. Police staff not assigned a dedicated extension will be provided with a personal voice mailbox associated with their badge number. All new and saved messages in the voicemail system will be automatically purged every 21 days.
- Departments are responsible for telephone equipment issued, and if phone equipment is damaged through neglect or misuse, the replacement cost will be charged back to the responsible department or employee.

O. Internet & Email Use Policy

- General use of the Internet through City equipment is a privilege, not a right and it may be revoked at any time for unacceptable use. The City retains the right to keep, retrieve and monitor all access to the Internet and related service activity.
- Incidental and occasional personal use of the Internet or the corporate email system is permitted, subject to the restrictions contained in this policy or any related City or departmental policy. Any personal use of internet or email is expected to be on the employee's own time and is not to interfere with the person's job responsibilities. Personal use of these systems must not detrimentally affect the job responsibilities of other employees, disrupt the system and/or harm the City's reputation.
- Please note, only the secure site(s) of http://webmail.appleton.org will be allowed to check your email using the internet from outside the City's local network.
- Maintain confidentiality by not forwarding or sharing any information that would violate the Data Protection Act or City guidelines.
- Delete any message received that were intended for another recipient. An incorrectly addressed message should only be forwarded to the intended recipient if the identity of the recipient is known and certain.
- Verify the recipient of the email is approved to receive the information contained in the email to avoid a breach of confidence.

The Information Technology Department reserves the right to:

- Restrict email storage space in the live (non-archive) email system.
- Delete any email older than 2 years that resides on the live email server.
- Restrict email size for both incoming and outgoing messages and attachments.
- Restrict the types of attachments in or out of the system to protect against viruses.

Every effort will be made to prevent Spam messages from being sent to your mailbox. Third party utilities may be required to accomplish this task. Any messages received that are determined to be Spam should be deleted by the end user and in no event should the

user attempt to respond to such senders.

P. Inappropriate use
    - Exercise due care when creating an email to avoid being rude or unnecessarily terse and ensure that your message meets the standards of professionalism the City expects of your position. Do not make any statements on your own behalf or on behalf of the City, which are intended or may defame, libel or damage the reputation of any person
    - Email Retention consists of all email sent or received through the City email system that has not been flagged as Spam. Such email will be archived for a period of seven years.

Q. Email Records Request Process:
    - All questions or requests made to the City of Appleton for viewing public record email messages should be sent directly to the City Attorney or records custodian of the respective department per the City's public records and retention guidelines.
    - Applicable fees as set by the State of Wisconsin may be charged to produce such information to the requestor.
    - Confidentiality-Email is not an inherently confidential or secure form of communication. You are expected to treat electronic information with the same care as you would paper-based information that is confidential. Keep all such information secure, use it only for the purpose(s) intended and do not disclose the same to any unauthorized third party (which may sometimes include other employees of the City).

R. Internet Filtering:
    - Access to certain web sites or categories to certain web sites may be filtered at the discretion of the Information Technology Department. In addition, certain ports, protocols, users, timeframes, URL addresses, and other items may be filtered or blocked.
    - You must not display, upload, download, use, retain, distribute or disseminate any images, text, materials or software which:

      Are, or might be considered offensive, abusive, indecent, obscene, pornographic or illegal, including content that is or could be considered to be a personal attack, rude or personally critical, sexist, racist, or generally distasteful. Encourage or promote activities that make unproductive use of City time.

      Involve activities outside of the scope of your responsibilities, for example, unauthorized selling/advertising of goods and services.

      Affect, or have potential to affect the performance, cause damage, or overload the City's system, network and/or external communications.

      Might be defamatory, incur liability on the part of the City, or adversely affect the image of the City.

      Would be a breach of copyright or license provision with respect to both programs and data.

Please note that any exceptions, due to job requirements, to the inappropriate use standards may be authorized by a Department Head with approval from the Information Technology Director.

The following activities are expressly forbidden:

The introduction of any form of computer virus.
Engaging in any activity that is illegal, distasteful or likely to have negative repercussions for the City.
Seeking to gain access to restricted areas of the network or other hacking activities.
Forgery or attempts to read other users' mail without their consent or permission.

Intranet

The City of Appleton Intranet, http://intranet, is intended to be viewed by internal network users only to improve communications among employees and departments. The Information Technology Department will maintain this internal website. It should remain the default web site for all Internet browsers and under no circumstances should confidential data be posted onto the intranet site.

If you are uncertain at any time how to apply any provisions this policy, you should seek guidance from your supervisor or the Information Technology Department prior to engaging in any activity covered in this document.