




INFORMATION TECHNOLOGY POLICY

Policy Title: 701 – COMPUTER AND TECHNOLOGY USE	Policy Number: APR 701
Effective: November 1, 2012	
Supersedes: APR #414 dated 11/97, revised 6/10	
Approval: 	Page 1 of 8

1. Scope

- | | |
|--|---|
| <input checked="" type="checkbox"/> Full-time | <input checked="" type="checkbox"/> Union |
| <input checked="" type="checkbox"/> Part-time | <input checked="" type="checkbox"/> Independent Contractors |
| <input checked="" type="checkbox"/> Temporary/Contract | <input checked="" type="checkbox"/> Visitors and Vendors |
| <input checked="" type="checkbox"/> Salaried | <input checked="" type="checkbox"/> Volunteers/Unpaid Interns |

Employees who are covered under the provisions of a collective bargaining agreement will follow the standards as contained in their respective contracts if this policy conflicts with the language in the contract.

This policy is applicable City-wide. All users of City computer and technology resources are expected to comply with this policy as a condition of continued employment or contracted services.

The provisions of this Policy are subject to, and may be superseded by (in the event of a conflict), relevant provisions of applicable collective bargaining agreements between the City and the various collective bargaining associations of the City

2. Purpose

The purpose of this policy is to outline the acceptable use of City of Ann Arbor computer and technology resources. These policies are in place to protect the employee, volunteer, City contractor, and the City. Inappropriate use exposes the City to risks including legal issues, compromise of network systems and services, and malicious cyber attacks.

2.1 Rationale

A large portion of City business is conducted with end-user technology resources, including Windows-based desktop and laptop computers, tablets, smart phones, and similar technologies. Protection of these resources and the information they handle is an essential part of doing business. Users have a critically important role to ensure that City technology resources are used in an appropriate and lawful manner.

3. Responsibilities

3.1 All users are responsible for:

- Knowing, understanding, and following all City policies
- Exercising good judgment and acting in a professional manner when using City technology resources
- Upon transfer to a new service area/unit, requesting that the authorities assigned to their User ID be changed to reflect the access requirements of the new job
- Immediately reporting security incidents such as their computer becoming infected with a virus

3.2 Management is responsible for:

- The actions of their staff, contractors, and volunteers and must ensure that all standards applicable to their environment are followed.
- Alerting Human Resources when a user transfers to a new service area/unit. The privileges assigned to the user's ID must be changed to reflect the access requirements of the new job.
 - Human Resource management is responsible for informing ITSU of the requested changes via a Helpdesk ticket.

3.3 Failure to comply with this policy is a violation of the City's Employee Standards of Conduct policy and may lead to:

- Revocation of system privileges
- Disciplinary action according to the City's Progressive Discipline policy

3.4 Failure to comply with this policy by a contractor using City technology resources may be considered grounds for breach of its contract and revocation of system privileges.

4. Policy

City technology resources (information, hardware, software, and infrastructure) must be used in an approved, legal, and ethical manner to protect the City from business risks.

4.1 Compliance and Enforcement

The City reserves the right to control, monitor and audit all uses of its technology resources. Inappropriate use of technology resources puts the City's network systems and services at risk from malicious cyber attack and/or exposes the City to legal liabilities. Actions that expose City information to capture, modification, and disclosure are grounds for disciplinary action.

4.2 Ownership and Business Use

All technology resources purchased by or licensed to the City are the property of the City.

The City reserves the right to remove unauthorized software found on any City technology resource, with or without notice.

The City reserves the right to remove from its information systems any material it views as offensive or potentially illegal.

City technology resources and similar City assets are provided for use by City employees (or other personnel) for legitimate City business purposes.

Reasonable personal use of City technology resources as defined by Service Area Administrators and Service Unit Managers is permitted, however the City reserves the right to block access to websites and manage connectivity as it deems appropriate.

4.3 Appropriate Use of City Technology Resources and Similar City Assets

City requirements must be followed for the appropriate use of City technology resources and similar City assets. Users must respect the rights of others when using City technology resources and similar City assets.

4.3.1 Prohibited Behavior

The following are examples of prohibited behavior. This list is not meant to be exclusive.

- Use of City technology resources to access, store, distribute or publish offensive content of any kind, including but not limited to pornographic material, hate mail and other offensive material.
 - An exception is made for Law Enforcement, 15th District Court, City Attorney, and Human Resources personnel only when handling this type of material is required in the course of their official City duties.
- Use of City technology resources or similar assets in support of a personal business, private consulting effort or similar venture, personal

political or lobbying activity, or for any illegal or other purpose that could cause harm to the City or otherwise adversely affect its interests.

- Use of City technology resources or similar assets in support of a charitable fund raising campaign without prior written authorization from the City Administrator and/or City Council.
- Loading, installing or storing non-City owned or sanctioned software or applications on City technology resources without express permission and/or authorization from ITSU. Such software includes but is not limited to, remote control software, unapproved instant messaging software (such as AIM, Google Talk, MSN, Yahoo Messenger, etc.), peer-to-peer file sharing software (such as Bittorrent, Limewire, etc.), shareware, open source software, public-domain software, and freeware.
- Using or accessing City resources that are not intended for the performance of their jobs. Access to a City technology resource does not imply permission to use the resource. For example, access to software installation packages on network drives does not imply that these can be installed. Software may require licenses and may not be installed without the purchase of those licenses.
- Examining, altering, copying, or deleting the files or directories of other users without owner permission or the appropriate authority.
- Knowingly entering false or inaccurate information into any City technology system.
- Misuse of system access privileges. Such misuse could include preventing legitimate authorized users access to City resources, or obtaining extra resources or access privileges without proper authorization.
- Unauthorized copying or distribution of system configuration files.
- Any other use that is illegal, violates City policy, or that could embarrass, offend, or harm the City, its employees, or its customers.
- Unauthorized moving of City desk phones from originally installed location. Moving a phone from its originally installed location can alter the 911 location data when calling 911 for an emergency. If a phone is moved it can report the wrong location to 911. All phone moves must be coordinated with the Help Desk

4.3.2 Required Behavior

- Users must report all information security alerts, warnings, suspected vulnerabilities, incidents and violations to management and ITSU through a helpdesk ticket.

4.4 Management of City Information

City Information is our most valuable City computing asset and must be appropriately protected from unauthorized access, modification, disclosure,

and/or destruction. Failure to properly manage information is a violation of City Policy.

4.4.1 The following basic principles must be followed for the management of City records and information:

- Information is an integral part of business and accountability.
- Information is a strategic business resource.
- Information created in the course of business is the City's property.
- Information quality is essential.
- Information management is everyone's responsibility.
- When a user is transferred or their employment is terminated, all information must be returned, transferred, or reassigned to another individual, User ID or area/group, to prevent the loss of City information and ensure ongoing ownership and control.
- City information, both hard copy and electronic files, must be managed and protected.

4.5 Risk Based Controls

- Controls are dependent on a risk assessment of the work environment.
- City technology resources must be protected in a manner commensurate with their sensitivity, value, and criticality or as required by law, contract, or operating agreement.
- In circumstances where application of an established control cannot be followed, compensating controls, authorized and approved by ITSU management, must be applied to mitigate the risk. Sound business judgment must govern this process.

4.6 Intellectual Property Controls

These controls protect the legal rights of the City. The City strongly supports and mandates strict adherence to software license agreements, copyright notices, and all applicable legal requirements.

- Reproducing, displaying, distributing or storing any materials that violate the trademark, copyright, licensing, or other intellectual property rights of any party, including the City, is strictly prohibited.
- Theft or misuse of technology resources, including unauthorized software copying or distribution, is prohibited and must be reported to the ITSU Director and Service Area Administrator immediately.

4.7 Hardware and Software Controls

ITSU must develop, follow and maintain inventory control procedures for software, hardware, and ancillary controls. When a user is transferred or their employment is terminated, all City-owned technology equipment including but not limited to desktop computer, laptop, mobile device, phone, printer, cables, software, and City information in the users' possession, must be returned to ITSU or reassigned to a new user and ITSU notified.

Where required by law or operating agreements, ITSU will develop the necessary control procedures in cooperation with the affected Service Area.

4.8 Hardware and Software Acquisition

Hardware and software must be procured in compliance with the Hardware, Software and IT Procurement policy.

4.9 Configuration Control

- Users must not change, modify or delete any configuration files or settings that will prevent, stop or interfere with the delivery of official City-approved patches, updates, security controls, or system enhancements.
- Updates and patches must be certified and tested for compatibility with the standard City computer operating system image prior to installation and must be obtained from official City sources. Users are not permitted to download or obtain these from non-City sources.
- All hardware upgrades to City-supplied technology resources must be performed by the ITSU Helpdesk or authorized City personnel.
- A City-configured computer operating system image must be installed on City supplied technology resources. Where the City-configured computer operating system image is not used, a clear business reason must be documented for using an alternate computer operating system image.
- The use of alternate computer operating system images must be approved by ITSU management prior to purchasing and deployment per the Hardware, Software, and IT Procurement policy.
- All proposed modifications to the City configured computer operating system image must be reviewed and approved by ITSU management prior to distribution or deployment. This includes but is not limited to, the installation of network services and protocols not included in the City configured computer operating system image.
- Whenever possible, the City configured computer operating system image with the latest security and encryption capability must be used to ensure the strongest security available.

4.10 Physical Security Controls

These controls protect technology resources, including digital media (CD, DVD, Memory Cards, USB drives, etc.), from theft, abuse, damage or unauthorized use.

- While off City premises or where there is a high risk of theft, technology resources, such as PC's, laptops, mobile devices, digital media, etc., must be securely stored when left unattended.
- Users must notify the ITSU Director and Service Area Administrator immediately if equipment is stolen, damaged, or missing.
- Equipment must not be relocated without Service Unit manager approval and ITSU Helpdesk notification.
- Except for assigned portable technology resources, equipment must not leave City premises without ITSU authorization.

4.10.1 Physical Security Guidelines

ITSU must be consulted before any of the following controls are used. These controls should be used where there is a high risk of theft, the power source is unstable, or static electricity is excessive. Local management must determine if these controls are required.

- Powering off desktop computer systems overnight.
- Using anchor pads or other approved security devices to physically secure computer systems.
- Marking computer systems with invisible identification to facilitate recovery if stolen.
- Installing power surge devices or using filtered power, when available, to protect internal circuits and prevent loss of data.

4.11 Backup Controls

These controls ensure that resources are available to restore normal operations after a business disruption.

- Official City records must not be stored exclusively on portable technology resources (Laptops, mobile devices, digital media, etc). The proper place for these files is on City network storage.
- ITSU will store or backup software according to software licenses agreements or local procedures.
- ITSU will store backup copies of production applications, data, and documentation in secure offsite locations.
- ITSU will develop and maintain a disaster recovery plan for City IT services.

4.12 Network Controls

- End-user computer systems must not be configured to function as servers without the express consent of ITSU. Prohibited behavior includes, but is not limited to, running server services or applications such as file, web, and database servers.
- Users must not establish electronic bulletin boards, local area networks, direct connections to other networks, Internet commerce systems, or other multi-user systems for communicating information on end-user computer systems without the express consent of ITSU.
- Network shares must be created on network servers, not personal computer systems and must be protected.
- Systems that automatically exchange data between devices, such as a Smartphone, tablet, or PDA and a personal computer, must not be enabled unless the systems have been evaluated and approved by ITSU management.

4.13 Electronic Communications (Email, instant messaging, etc.)

- All users are expected to be familiar with, and fully comply with the Electronic Communications policy and applicable City record retention policies.

4.14 Public Internet

- All users are expected to be familiar with, and fully comply with the Public Internet policy.

4.15 Information Security

- All users are expected to be familiar with, and fully comply with the Information Security policy.

4.16 Hardware, Software, and IT Procurement

- All users are expected to be familiar with, and fully comply with the Hardware, Software and IT Procurement policy.