



City of Ann Arbor

Information Technology Policy Manual

TABLE OF CONTENTS

City-Wide Information Technology Policy Manual Overview	3
1.1 Information Technology Policy Manual Introduction	3
1.2 Rationale.....	3
1.3 Goals	3
1.4 ITPM Architecture	3
1.5 ITPM Compliance and Responsibilities.....	3
1.6 Information Technology Policy Governance	4
1.7 ITPM Deployment	5
1.8 Definitions	5
Revision History	6
Information Technology Policies, Procedures, and guidelines	7
701 – Computer and Technology Use.....	8
702 – Electronic Communications.....	16
703 – Public Internet	22
704 – Information Security	27
705 – Hardware, Software and IT Procurement.....	32
706 – Password Policy.....	35
707 – General IT Communications Guidelines.....	39
708 – Archive and Data Retention Process	41
709 – Scheduled and Unscheduled Systems Maintenance Procedure and Communications Plan	46
710 – On-Site Vendor/Guest Visitation	49
711 – Remediation/Destruction of Digital Media	51
712 – Onboarding and Termination of Users’ Computer Access	53
713 – Power Testing for Data Centers	56
714 - Email Signature Policy	57
715 – Media Protection Policy.....	60
716 – Artificial Intelligence (AI) Usage Policy	64
Glossary.....	70

CITY-WIDE INFORMATION TECHNOLOGY POLICY MANUAL OVERVIEW

1.1 INFORMATION TECHNOLOGY POLICY MANUAL INTRODUCTION

The Information Technology Policy Manual (ITPM) defines a set of policies that all City employees, third-party providers, consultants, volunteers, and temporary employees must adhere to when utilizing City of Ann Arbor information technology resources. The policies contained within the ITPM have been developed to ensure that all users are aware of the roles, responsibilities, and appropriate use surrounding City of Ann Arbor technology resources. Inappropriate use of technology resources can put the City's networks, systems, and services at risk from cyber-attack, expose the City to legal liabilities, and put the City's reputation in jeopardy.

Exceptions to information technology policies may exist in rare instances where existing technology prevents compliance or a compliant solution is not financially feasible. These exceptions must be approved by ITSU management. Risks associated with non-compliance issues must be accepted and assumed by Service Area/Service Unit management.

1.2 RATIONALE

The ITPM was developed to provide clear IT policy to City of Ann Arbor employees.

1.3 GOALS

- Develop a standard IT policy manual, containing all IT policies
- Enhance non-IT professional readability and understanding
- Implement a sustainable governance model around the IT policies
- Incorporate City-specific content into new IT policy manual where applicable
- Introduce the new/updated IT policies

1.4 ITPM ARCHITECTURE

The ITPM will be the definitive source for IT policies. All IT-related guidelines and procedures will be maintained by the Service Areas/Service Units that created them.

1.5 ITPM COMPLIANCE AND RESPONSIBILITIES

The goal of the ITPM is to minimize risks and protect individuals as well as the City. All employees, permanent, temporary and contract, as well as contract, agency, volunteers and third party providers must adhere to the following rules:

Definition of Non-Compliance

- Non-compliance means the conduct of any employee which is not supportive of IT policies.

Examples of non-compliance include, but are not limited to, the following:

- Employees are negligent in applying appropriate security and controls within the organization supported
- An employee's action or inaction contributes to a violation
- An employee does not immediately resolve or escalate issues when appropriate
- Employees fail to take appropriate action in response to a complaint or an incident

Roles and Responsibilities

Employees:

- Understand, implement and follow applicable policies
- Monitor and address issues
- Resolve and/or escalate issues

Supervisors / Managers:

- Monitor their work areas for compliance and address any incident(s) of noncompliance
- Follow processes for escalating issues
- Intervene immediately to stop all non-compliance activities

1.6 INFORMATION TECHNOLOGY POLICY GOVERNANCE

Information Technology Leadership Board (ITLB)

The ITLB is comprised of the Information Technology Director (chair), City Administrator, City Attorney, 15th District Court Administrator, Service Area Administrators or their designees, and the Human Resources Director.

The ITLB will:

- Review and approve all policy changes
- Provide guidance on policy modifications for intent and scope
- Decide if awareness efforts must take place before the policies are issued or, if the update warrants a general notice and explanation to employees, inclusion in the A2 News Notes newsletter

When policy-related issues or the need for policy changes arise, the ITLB will be consulted as needed. A subset of the ITLB will be assembled based upon the subject matter of the issue to discuss and make a recommendation or ruling on the issue.

1.7 ITPM DEPLOYMENT

Unless another format is required by collective bargaining agreements (“CBA”), The ITPM will be presented via the City’s internal website (A2Central) with several different views. This website will be the single point of resource with key contacts, changes to IT Policy, and downloads of the policy manual.

1.8 DEFINITIONS

For purposes of the ITPM the following definitions shall apply:

Policy	Policies are high-level management statements, instructions or business rules that provide guidance to enable individuals to make present and future decisions. Policies are mandatory. Special ITSU management approval is required when anyone wishes to take a course of action that is not in compliance with policy.
Guidelines	Guidelines are recommended best practices that satisfy a policy, standard, or a control. While guidelines are not mandatory they are strongly recommended and must be implemented wherever possible.
Procedure	Procedures are specific operational steps or manual methods that support a policy or a standard.

REVISION HISTORY

REVISION NUMBER	DATE	REASON FOR REVISION	REVISED BY
1.0	March 2012	Initial draft document	IT Policy Focus Group / ITSU
1.1	May 2012	Legal review	City Attorney's Office/HR
1.2	June 2012	Final draft	ITSU
1.3	July 2015	Guideline – 706, 707, 708	Tom Shewchuk
1.4	December 2018	Update to include 709-713	Jen Grimes
1.5	March 2022	Revision to 712	Jen Grimes
1.6	April 2022	Revision to 712	Jen Grimes
1.7	June 2022	Revisions to 702, 706, and 709	Jen Grimes
1.8	January 2024	Revisions to 701	Jen Grimes

INFORMATION TECHNOLOGY POLICIES, PROCEDURES, AND GUIDELINES

The City of Ann Arbor IT Policies have been developed to ensure that all users are aware of the roles, responsibilities, and appropriate use of City-owned technology resources.



INFORMATION TECHNOLOGY POLICY

Policy Title: 701 – Computer and Technology Use	Policy Number: APR 701
Effective: January 22, 2024	
Supersedes: version from November 2012	
Approval: Tom Shewchuk	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 moved 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.
- Users are expected to ensure their desktop or laptop computer is powered on and connected to the City network (either by physical location or VPN software) for a minimum of 8 hours weekly, with several of those hours at 3pm or later. Failure to do so prevents the ability of maintaining current security updates and patches.

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.



INFORMATION TECHNOLOGY POLICY

Policy Title: 702 – Electronic Communications	Policy Number: APR 702
Effective: July 13, 2022	
Supersedes: Revision November 2012	
Approval: <u>Tom Shewchuk</u>	Page 1 of 6

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 electronic communication systems 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 define the acceptable use standards and control requirements for City electronic communication systems, including but not limited to: email, instant messaging (IM), and text messaging.

2.1 Rationale

Electronic communications, including email, instant messaging (IM), and text messaging, can be intercepted, forwarded, printed, or stored by others.

Under certain conditions, electronic communications remain retrievable when a traditional paper communication would have been discarded or destroyed in the normal course of business. Employees must be aware that topics covered in electronic communications sent through City systems could disclose sensitive or inappropriate information which could breach City security measures, cause the City public embarrassment, or financial loss.

3. Responsibilities

3.1 Electronic Communications users are responsible for:

- Being familiar with and fully complying with this policy
- Exercising due care when using City electronic communication systems
- The management, retention, disposal and classification of their electronic communications consistent with adopted City record retention policies

3.2 Management is responsible for:

- Periodically reviewing the electronic communications accounts that they are responsible for and requesting that ITSU remove those accounts that are no longer required
- Alerting Human Resources of the termination of an employee and requesting that their electronic communications accounts be disabled and if necessary, their contents retained and/or access transferred to the appropriate authorized City personnel
 - Human Resource management is responsible for informing ITSU of the requested changes via a Helpdesk ticket.

3.3 ITSU is responsible for:

- Classifying electronic communications users with the correct employment type
- The management, retention and disposal of backup or archived electronic communications on City servers

3.4 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

3.5 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 electronic communication systems, including but not limited to: email, instant messaging (IM), and text messaging are provided for use by City employees (or other personnel) for legitimate City business purposes.
- Personal accountability is mandated for user electronic communications accounts. Passwords used to access electronic communications must not be shared.

4.1 Acceptable Use

- Personal non-City electronic communications accounts must not be used for the generation of City records.
- Email communications should always be handled inside of City provided a2gov.org email systems and City business should not be conducted in outside email systems.
- Accessing, reproducing, displaying, distributing or storing any materials that are sexually explicit, obscene, defamatory, harassing, illegal, or otherwise inappropriate is strictly prohibited.
 - 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.
- All City electronic communications must be consistent with the City's HR Employee Standards of Conduct policy.
- Without prior written authorization from the City Administrator and/or City Council, City electronic communication systems must not be used for charitable fund raising campaigns.
- City electronic communications may not be used for political advocacy efforts, religious efforts, private business activities, distributing chain mail, propagating hoaxes, or other purpose that could cause embarrassment to the City or otherwise adversely affect its interests or violate federal or state laws.
- News feeds, email lists, RSS feeds, and other mechanisms for receiving information over the Internet must be restricted to material that is clearly related to both City business and the duties of the receiving user. Users are reminded that the use of City technology resources must never create the appearance or the reality of inappropriate use.
- Misrepresenting, obscuring, suppressing, or replacing another user's identity on an electronic communications system is prohibited. The user name, electronic communications address, organizational affiliation, and related information included with electronic communications must reflect the actual originator of the messages or postings.
- With the exception of City-sanctioned electronic communications systems (IT system maintenance notices, list servers, etc) that are

intended to be anonymous, sending anonymous electronic communications is strictly prohibited.

4.2 Electronic Communications Content

- Offensive material must not be forwarded or redistributed to either internal or external parties, unless this forwarding or redistribution is in connection with your official City-assigned work duties or is being sent to the City Human Resources Service Unit or City Attorney's Office in order to assist with the investigation of a complaint.
- Electronic communications content should not be altered and then forwarded without the permission of the originating sender. If content is altered to remove sensitive information, it must be clearly indicated in the new message. Altering the content to change the intention of the originator is strictly prohibited.
- Despite the best efforts of the City, electronic communications systems may deliver unsolicited messages that contain offensive content. The City is not responsible for the content of material viewed, downloaded or received through the Internet.

4.3 Electronic Communications Management

- Database files, used by City electronic communication systems are archived on City servers for disaster recovery purposes and will be deleted at periods chosen by ITSU but not to be less than six weeks.
- Electronic communications content which documents a decision, action or transaction is considered an official City record and must be managed and retained according to the City's Records Retention policies.
- Electronic communications inboxes are not intended to be repositories for official City documents or other important business-related correspondence. Users must regularly move these correspondences to word processing documents, databases, or other electronic file storage areas located on the City Network that are intended for storing official documents.

4.4 Malware and Viruses

- All email that leaves or enters the City networks will be scanned for malware (viruses, worms, etc.) by ITSU.
- Users must not click links or download attachments contained within electronic communications coming from unknown sources. If assistance is needed to determine an electronic communication's legitimacy, contact ITSU Security and Controls through the Helpdesk.

4.5 Phishing (Fraudulent) Messages

- Users must immediately delete “phishing” (fraudulent) electronic communications messages that ask for sensitive information. If assistance is needed to determine an electronic communication’s legitimacy, contact ITSU Security and Controls through the Helpdesk.
- Users must not click links or download any attachments within phishing (fraudulent) electronic communications messages.

4.6 Encryption

- By default, electronic communication is an unsecure platform and is not suitable, by itself, for sending sensitive information. An electronic communications message assumes the classification of the data contained in the message and therefore sensitive information must only be sent via electronic communication if it is appropriately protected using the City’s encryption services.
- ITSU will identify and provide a method for encrypting sensitive outgoing electronic communications that require additional protection because of their content.

4.7 Electronic Communications Forwarding

- Automatically forwarding electronic communications from a City electronic communications account to a public electronic communications system is prohibited without written permission from ITSU since the contents of the electronic communications, including attachments, can be forwarded, intercepted, printed, and stored by unauthorized parties.
- ITSU cannot guarantee that public electronic communications systems are private with access limited to only the intended recipients(s).

4.8 Broadcasts and Alerts

- “All user” email broadcasts or mass electronic communications are not permitted except by permission of the City Administrator.

4.9 Delegate Authority


- Electronic communications must not be read or sent from another user’s account, except under proper delegate arrangements.
- Generic User IDs should be used for electronic communications only when it is impractical to use personal User IDs. When a generic User ID is used, all other users of the generic account must be given delegate access to the functions that they require.

4.10 Third Parties

- Vendors wishing to communicate electronically with the City must use their own electronic communications systems.
- Contractors operating in direct support of City business operations may use City electronic communications systems. In these cases, requests for use of City electronic communications systems and deviations from prescribed functionality must be reviewed and approved by ITSU management with recommendation from their contract administrator.



INFORMATION TECHNOLOGY POLICY

Policy Title: 703 – Public Internet	Policy Number: APR 703
Effective: November 1, 2012	
Supersedes: APR #414 dated 11/97, revised 6/10	
Approval: 	Page 1 of 5

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 ensure the appropriate use of the Public Internet and to protect the integrity and availability of City networks.

2.1 Rationale

The Public Internet is an open communication network that serves billions of users worldwide. The Public Internet facilitates business transactions, communication with the public, and provides resources to conduct

research. As such, the power of the Public Internet can be harnessed to provide significant benefits for City business. Conversely, it can present a number of risks if not sufficiently controlled. These risks include breach of security, damage to reputation, lost productivity, legal liability, damage to systems and data, increasing network traffic, etc.

Users must evaluate the importance and sensitivity of any data to be transmitted via the Public Internet, including electronic communications. The objective of this policy is to mitigate risks by ensuring users are aware of their obligations when using the Public Internet via the City's computing systems.

3. Responsibilities

3.1 All users are responsible for:

- Being familiar with and fully complying with this policy
- Ensuring that City information is protected per IT policy requirements (*the City does not automatically protect information sent via the Public Internet*)

3.2 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

3.3 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

Access to the Public Internet is provided for use by City employees (and other authorized personnel) for legitimate City business purposes.

4.1 Accountability & User Identity

- Users are accountable for their actions when accessing the Public Internet using the City network and/or with City computing resources.
- Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Public Internet or any City electronic communications system is prohibited.
- The use of anonymous proxies or other anonymous facilities are not permitted.

4.2 External Site Access

- The ability to access a specific Public Internet website does not in itself imply that users of City systems are permitted to visit that site. The City may, at its discretion, restrict or block access to Public Internet sites and/or services and prevent the downloading of certain file types.

4.3 Public Internet Connections

- All communications between a City network and any non-City network must use solutions approved by ITSU management and use network suppliers chosen by the City.
- Service Units are prohibited from procuring unapproved dedicated connections to the Public Internet without the documented approval of ITSU management.
- All communications between City-owned equipment on City premises and any other non-City network (such as the Public Internet) must use solutions approved by ITSU management, which are secured with appropriate administrative and technical controls.

4.4 Appropriate Use of City-provided Public Internet access

4.4.1 City requirements for the appropriate use of City-provided Public Internet access.

- The City is not responsible for the content that users may encounter when they use the Public Internet.
- Users who discover they have connected with a website that contains sexually explicit, racist, sexist, violent, or other potentially offensive material must immediately disconnect from that site.
- Privileged and confidential City information must only be revealed on the Internet if the information has been officially approved for public release per the City's Communications Guidelines.

4.4.2 Improper use of the Public Internet, City Intranet, electronic communications, and other Public Internet services is prohibited. Improper use includes but is not limited to:

- Accessing, reproducing, downloading, transmitting or possessing any materials that are sexually explicit, obscene, defamatory, harassing, illegal, or otherwise inappropriate
- Accessing, creating, downloading, transmitting or possessing offensive, defamatory, threatening or abusive messages in any way, including through the Public Internet
- Transmitting 'jokes' of an offensive nature, for example, content which is sexually explicit, racially offensive or otherwise demeans

people on the basis of their religion, disability, sexual orientation or any other protected attribute

4.5

Privacy and Legal Rights

- The City reserves the right to conduct random audits of its technology resources to identify non-compliance with policies and to monitor or access files, Public Internet usage history, and the contents of electronic communications including but not limited to: email, instant messaging (IM), and text messaging sent through or stored on City technology resources.
- Employees (and other authorized personnel) do not and should not have any expectation of privacy in their use of City-owned technology resources or the contents of any electronic communication or file, both business and personal, sent through or stored on City technology resources.
- Technical support personnel are prohibited from reviewing the content of an individual user's electronic communications out of personal curiosity or at the request of individuals who have not gone through proper approval channels. Written approval from the City Administrator, City Attorney, Chief Judge, a Service Area Administrator, and/or the Human Resource Director is required prior to any monitoring or review of electronic communications.
- Intellectual Property Rights, such as copyrights, patents, and trademarks must be respected. Users using City Public Internet systems must repost or reproduce material only after obtaining permission from the source or quote material from other sources only if these other sources are properly identified.

4.6 Encryption

- Confidential personal information and information that can be used to gain access to goods, services, or computer resources must not be sent over the Public Internet in readable form. Proper encryption must be used. This type of information includes credit card numbers, Social Security numbers, driver's license numbers, logon passwords, etc.
- Protection mechanisms such as secure Internet connections (<https://>) or other City-approved encryption techniques can be used to protect sensitive information. Contact ITSU if assistance is needed to determine proper protection methods for sensitive information.
- Whenever encryption is implemented, City-approved encryption methods must be used. The use of all other encryption methods is not permitted.

4.7 Virus Checking

- All files downloaded from City or non-City sources, such as the Public Internet, will be automatically scanned with current ITSU-supplied virus detection software.

4.8 Public Internet Services


- The use of any Public Internet (AKA “Cloud”) service must be reviewed and approved by ITSU management. The risk associated with the service must be identified and appropriate controls to minimize the risk must be defined and implemented. An ITSU staff member must be included in the development of any business case and process.
- Use of a Public Internet service for other than its intended purpose is considered an abuse of the service and is subject to termination of the right to use the service.

4.9 Management Review

- At any time and without prior notice, City management reserves the right to examine electronic messages, files stored on City-owned technology resources, web browser history/cache files, web browser bookmarks, logs of web sites visited, computer system configurations, and other information stored on or passing through City systems.



INFORMATION TECHNOLOGY POLICY

Policy Title: 704 – Information Security	Policy Number: APR 704
Effective: November 1, 2012	
Supersedes: APR #414 dated 11/97, revised 6/10	
Approval: 	Page 1 of 5

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 protect the integrity and availability of City information and to protect City technology resources from unauthorized use or modification and from accidental or intentional damage or destruction.

2.1. Rationale

Information and technology resources are relied on for an increasing number of critical City business tasks. Threats from hackers and malicious software

continue to increase at an exponential rate each. In order to protect the City's information and technology resources from such threats, an appropriate level of information security must continually be developed, implemented, and maintained.

The information security objectives of the City are critical to the success of the City's governance and service missions. The success of the information security program depends on strong support from all users throughout the City. Everyone is responsible for security.

3. Responsibilities

3.1. All Users are responsible for:

- Protecting their accounts and privileges
- Keeping passwords private. City employees, and all other persons subject to these policies are prohibited from sharing their passwords with another person.
- Accepting personal accountability for all activities associated with the use of their user accounts and related access privileges
- Ensuring that their use of City computers, electronic communications, networks, and Internet access is restricted to authorized purposes and defined use limitations
- Maintaining the confidentiality of sensitive information to which they are given access privileges
- Reporting all suspected security and/or policy violations to the appropriate authority (e.g. Service Area Administrator, Service Unit Manager, and/or ITSU through the Helpdesk)

3.2. Management in each Service Area/Service Unit, in cooperation with ITSU, is responsible for:

- Monitoring work areas for compliance and address any incident(s) of noncompliance

3.3. ITSU is responsible for:

- Supporting the need for appropriate security controls within the IT environment
- Supporting information security awareness and education program efforts
- Providing direction and support for the continual development, implementation, and maintenance of City-wide information security policies, programs, and procedures
- Providing information as necessary to the City about existing and emerging legal and compliance requirements and about best practices associated with information systems security
- Reviewing exceptions to this policy to ensure their appropriateness and legality

- Acting as an advocate for budget and resource requests related to ensuring the maintenance of effective information security programs

3.4. 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

3.5. 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

It is the policy of the City of Ann Arbor to protect City of Ann Arbor information in accordance with all applicable laws, governmental regulations, and accepted best practices to minimize information security risk; ensuring the right information is available to the right people at the right time.

4.1. Information Security Program Oversight

To achieve the information security goals of the City of Ann Arbor, the Ann Arbor Information Technology Leadership Board (ITLB) authorizes the City of Ann Arbor IT Director to develop and maintain the City of Ann Arbor Information Security Program and requires all Service Areas and Service Units to comply.

The Information Security Program will consist of the Information Security policies and Information Security awareness training for employees.

4.2. Security Incident Handling

- Users must immediately report security incidents, such as their computer becoming infected with a virus, to the ITSU Helpdesk.
- If any user of City technology resources believes for any reason that their credentials (User ID and password, token, etc.) have been compromised or misused, they must immediately shut down the involved computer, disconnect from all networks, and report the event to the ITSU Director and Service Area Administrator.
- ITSU is the only unit authorized to broadcast information about computer security alerts and determine the appropriate action in response to such notices. Users must not propagate or forward any virus notification messages except to ITSU for examination.

4.3. Access Controls

These controls protect data from unauthorized disclosure, modification or loss.

- Access to information must be based on a need to know and is controlled.
- Users are responsible for all actions taken with their personal user accounts (User IDs).
- Users must inform Service Unit management about any excessive access privileges they may hold, and ask that they are removed (if not expressly required for their position). For example, if a user changes jobs into a new service area/unit, access to the old service area/unit's data may need to be curtailed.
- Passwords used to access City systems must meet City password standards.
- Other than public-use, kiosk, and related computers, all City workstations will be set to automatically lock after a pre-defined period of inactivity requiring that the user enter their password to unlock the system.

4.4. Software

- Virus detection software, provided by ITSU, must be installed, functional and updated on PCs, laptops, and similar devices.

4.5. Network Controls

- To protect the security and integrity of City networks, users are not permitted to connect non-City owned technology resources to private, internal City networks without permission from ITSU. Such equipment includes but is not limited to: personal PCs, laptops, printers, mobile devices (phones, tablets, handhelds, etc.), and networking equipment (wireless access points, routers, switches, etc.).
→ *Note: The term 'connect' is intended to include both wired and wireless connections.*
- All access to or from City networks must be via ITSU management-approved telecommunication solutions. The use of modems and the private installation of data or voice lines, either fixed or wireless, is prohibited without explicit authorization from ITSU.
- All inbound connections to the City's internal networks require a City-approved virtual private network (VPN) software package.
- The presence of any active secondary network connection on a computer that is attached to the City network is not permitted.

4.6. Security Tampering

- Testing or probing the security mechanisms of any City or non-City system, or the possession or usage of tools for detecting information system vulnerabilities, or tools for compromising information security mechanisms,

are prohibited without the advance permission of the Director of Information Technology.

- Maliciously degrading or disrupting the performance or services of any technology resource or network (both City owned and non-City owned) is prohibited.

4.7. Management of City Information


- City information, both hard copy and electronic files, must be managed and protected.
- Citizen and employee personal information must not be shared with unauthorized individuals.
- Information must be protected with due care and due diligence regardless of the computing platform. For example, if the Payroll department downloads online payroll information from an application to their PCs for spreadsheet (Excel) manipulation and report, it must be protected in a similar manner to the information that is stored on City servers. There must be adequate access controls to ensure that the information is only accessible by those individuals with a need to know.
- Encryption requirements must be followed for information stored on end-user technology resources, digital storage media (such as memory cards, CDs, DVDs, USB based storage devices, etc.) or online providers.
- Privileged and confidential City information must only be revealed on the Internet if the information has been officially approved for public release per the City's Communications Guidelines.

4.8. Technology Disposal

- Technology resources (computers, copiers, mobile devices, etc) or digital storage media removed from service or the City environment (end of lease, sale, recycling, disposal, etc.) must be securely disposed of through ITSU only.



INFORMATION TECHNOLOGY POLICY

Policy Title: 705 – Hardware, Software and IT Procurement	Policy Number: APR 705
Effective: November 1, 2012	
Supersedes: APR #414 dated 11/97, revised 6/10	
Approval: 	Page 1 of 3

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 City personnel who have responsibilities that include the evaluation or purchase of new hardware, software or IT services must follow the requirements of this policy.

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 control the process of acquiring computer hardware, software and IT services to ensure that appropriate platforms are provided to support business applications.

2.1 Rationale

Without formal procurement policy and processes, the City may be exposed to several business risks, which include not benefiting from economies of

scale when different groups purchase hardware, software or IT services in isolation, non-standard technology, use of unauthorized software, and inappropriate contracts. All of these risks lead to increased costs and potentially severe business consequences.

3. Responsibilities

All City personnel who have responsibilities that include the evaluation or purchase of new hardware, software or IT services must follow the requirements of this policy.

4. Policy

4.1 Technology Standards

- Hardware, software or IT services must be procured in compliance with City IT standards.
- Hardware, software or IT services must be standardized to reduce complexity and cost to procure, maintain, and support the technology.

4.2 Procurement Control

- Software must be either developed in-house, or obtained from legitimate and reliable third parties.
- Products must be reviewed and tested prior to their use and financial settlement.
- Selection of IT services must be performed by the Information Technology Service Unit in conjunction with the requesting Service Unit.

4.3 Hardware, Software and IT Services Acquisition

- City purchasing procedures must be followed in the procurement of information technology related hardware, software and IT services.
- All purchase requests that include non-standard hardware, software, or service components must be reviewed and approved by designated ITSU management personnel.
- All software and hardware is to be procured through the IT Service Unit except where an alternate procurement agreement between ITSU and the service unit exists.
- All agreements with IT Service Providers must be authorized by the IT Service Unit, in conjunction with the requesting Service Unit.
- Acquisition, and use of Public-Domain software, freeware, shareware, open source software, or software downloaded from the Internet, is prohibited without written pre-approval from the ITSU management.

- Any non-disclosure agreement required must be approved by the City Attorney's office.

4.4 Intellectual Property Rights and Licensing

- All copyright and/or licensing requirements must be followed per the requirements in the Intellectual Property Policy.
- Proof of ownership and license must be maintained for all software, as long as the software is in use. Records documenting end of use and disposal should also be maintained.
- The IT Service Unit will maintain records for all hardware, software and IT service purchases made

4.5 Third Party Software Maintenance

- For licensed software acquired from third parties, the third parties must have appropriate procedures to validate, protect and maintain the software product's integrity rights.
- Consideration should be given to the support of the product in a maintenance agreement related to the delivered product.



INFORMATION TECHNOLOGY POLICY

Title:	706 – Password Policy	Policy Number:	APP 706
Effective:	July 13, 2022		
Supersedes:	December 14, 2018		
Approval:	Tom Shewchuk, IT Director	Page	1 of 2

1.0 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 Citywide. 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

2.0 Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of the City of Ann Arbor's resources. All users, including contractors and vendors with access to the City of Ann Arbor systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

3.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

4.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any City of Ann Arbor facility, has access to the City of Ann Arbor computing network, or stores any non-public City of Ann Arbor information.

5.0 Policy

5.1 General

5.1.1 Password Aging

All City of Ann Arbor employees (fulltime, part-time and temporary) will be required to change their passwords every 90 days when logging onto the City of Ann Arbor computing network.

5.1.2 System Administrator Passwords

All system-level passwords (e.g., root, domain administrator, application administration accounts, etc.) must be changed promptly after a staff member who had administrative level access to City IT computing assets leaves the organization.

5.1.3 System Administrator Password Protection

All production system-level passwords used by Information Technology staff must be stored in a separate, secure system for password management (e.g. KeePass).

User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

All employees with a network password, as well as individuals with system-level passwords, must conform to the guidelines described below for all City of Ann Arbor employees accessing the City's computing network.

5.2 Guidelines

5.2.1 General Password Construction Guidelines

All users at The City of Ann Arbor should be aware of how to select strong passwords. Strong passwords have the following characteristics and must be constructed using the criteria below:

- **Minimum Password Length** determines how short passwords can be. The minimum password length is fifteen (15) alphanumeric characters.
- **Password Complexity Requirements** determines whether password complexity is sufficient. User passwords must meet the following requirements:
 - The password contains characters from at least three of the following four categories:
 - English uppercase characters (A - Z)
 - English lowercase characters (a - z)
 - Base 10 digits (0 - 9)

- Non-alphanumeric (For example: !, \$, #, or %)
- **Password History** determines the number of unique new passwords a user must use before the user may reuse a prior password. Password history is set at 10 for all City of Ann Arbor employees.

5.2.2 Weak Passwords

Weak passwords will no longer be allowed for logging onto the City's computing network. Weak passwords exhibit the following characteristics:

- The password contains less than eight characters;
- The password is a word found in a dictionary (English or foreign);
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "The City of Ann Arbor" or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

5.2.3 Password Protection Standards

- Passwords should not be shared unless explicitly approved by a manager as part of an approved business process. The IT Director should also be notified when this is necessary. If someone demands access to a password for which they are not explicitly approved, refer them to this document and direct them to the Information Technology Services Unit.
- Always decline the use of the "Remember Password" feature of applications. If an account or password compromise is suspected, report the incident to the Information Technology Services Unit.
- Always use different passwords for City of Ann Arbor accounts from other non-City of Ann Arbor access (e.g., personal ISP account, option trading, benefits, etc.).
- Always use different passwords for various City of Ann Arbor access needs whenever possible. For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.
- Do not share the City of Ann Arbor passwords with anyone, including administrative assistants, secretaries, co-workers or supervisors. All passwords are to be treated as sensitive, confidential information.
- Passwords should never be written down or stored on-line without encryption.

- Staff should not reveal passwords in email, chat, or other electronic communication. System administrators may provide initial or reset passwords electronically, but they will do so via secure means such as encrypted email or Microsoft Teams communications.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action up to and including discharge. Password cracking or guessing may be performed on a periodic or random basis by the Information Technology Services Unit or its delegates in order to ensure the security of the system. If a password is guessed or cracked during these exercises, the user/owner will be notified and will be required to change it immediately.



INFORMATION TECHNOLOGY POLICY/PROCEDURE/GUIDELINES

Title:	707 – General IT Communications Guidelines	Document Number:	707
Effective:	July 13, 2022		
Supersedes:	June 30, 2015		
Approval:	Tom Shewchuk, IT Director	Page	1 of 2

1. Purpose

The purpose of this policy is to set standards for communications within the IT department. Proactive and efficient communications is desired, use of current productivity applications is encouraged and excessive and unnecessary communications should be limited as schedules change.

1.1. Rationale

- 1.1.1. Due to the nature of our work IT employees schedules change frequently and it is imperative that when an IT resource is needed their status and whereabouts can easily be determined so the appropriate method of communications can be utilized.
- 1.1.2. Planned activities do not need to be communicated or pushed to the IT staff. If an IT staff member needs to learn the status of another IT staff member they should reference Outlook to determine their whereabouts.
- 1.1.3. Unplanned or emergency situations should be proactively communicated to the IT staff.
- 1.1.4. The following methods of communications are available to IT staff: email, city phone, cell phone, , Microsoft Teamstext, etc...

1.1.5.As always, discretion should be used given the criticality of the situation.

2. Responsibilities

2.1.All IT Department staff will utilize the following guidelines for scheduling and communicating planned and unplanned staff activities:

Planned:

- Keep their Outlook calendar updated at all times
- Share their calendar with all IT staff and give access to view the detail of the appointment(s)
- If an IT staff member does not wish others to view the details of their appointment(s) they must mark the appointment private
- Long-term vacations leave should be communicated to all IT staff 3 days in advance to allow for any knowledge sharing

Unplanned:

- Proactively communicate to all IT staff in the case of an emergency, sickness, last minute changes, etc...

Other situations:

2.1.1. Utilize good judgement and discretion as necessary

2.2.IT Department Management

2.2.1.Monitoring work areas for compliance and address any incident(s) of noncompliance



INFORMATION TECHNOLOGY POLICY/PROCEDURE/PROCESS

Title:	708 – Archive and Data Retention Process	Document Number: 708
Effective:	February 10, 2021	
Supersedes:	July 7, 2015	
Approval:	Tom Shewchuk, IT Director	Page 1 of 5

1. Purpose

Develop a process for archiving and data retention for a city asset upon separation of an employee.

1.1. Rationale

- While employed with the City all city-related data generated by the employee should be stored on the City's network or City's cloud resources.
- All city-related network data must be backed up and (or) archived per this process and the State of Michigan data retention schedule.

2. Responsibilities

2.1. New Process (Non-Temporary Employees)

1. Employee or employee's manager advises HR of the employee separation.
2. HR emails the department manager a "Manager IT Separation Form" and letter with instructions for the department manager to follow before the employees last day (see Appendix A)
3. Department manager fills out the Manager IT Separation Form electronically and emails it to HR within 5 working days from receiving the initial email.
NOTE: The process cannot start without the completed Manager IT Separation Form.
4. HR submits a Help Desk ticket and attaches the Manager IT Separation Form. If this is an urgent or sensitive separation, HR can email, phone, or visit the Help Desk and request this process be followed in a more

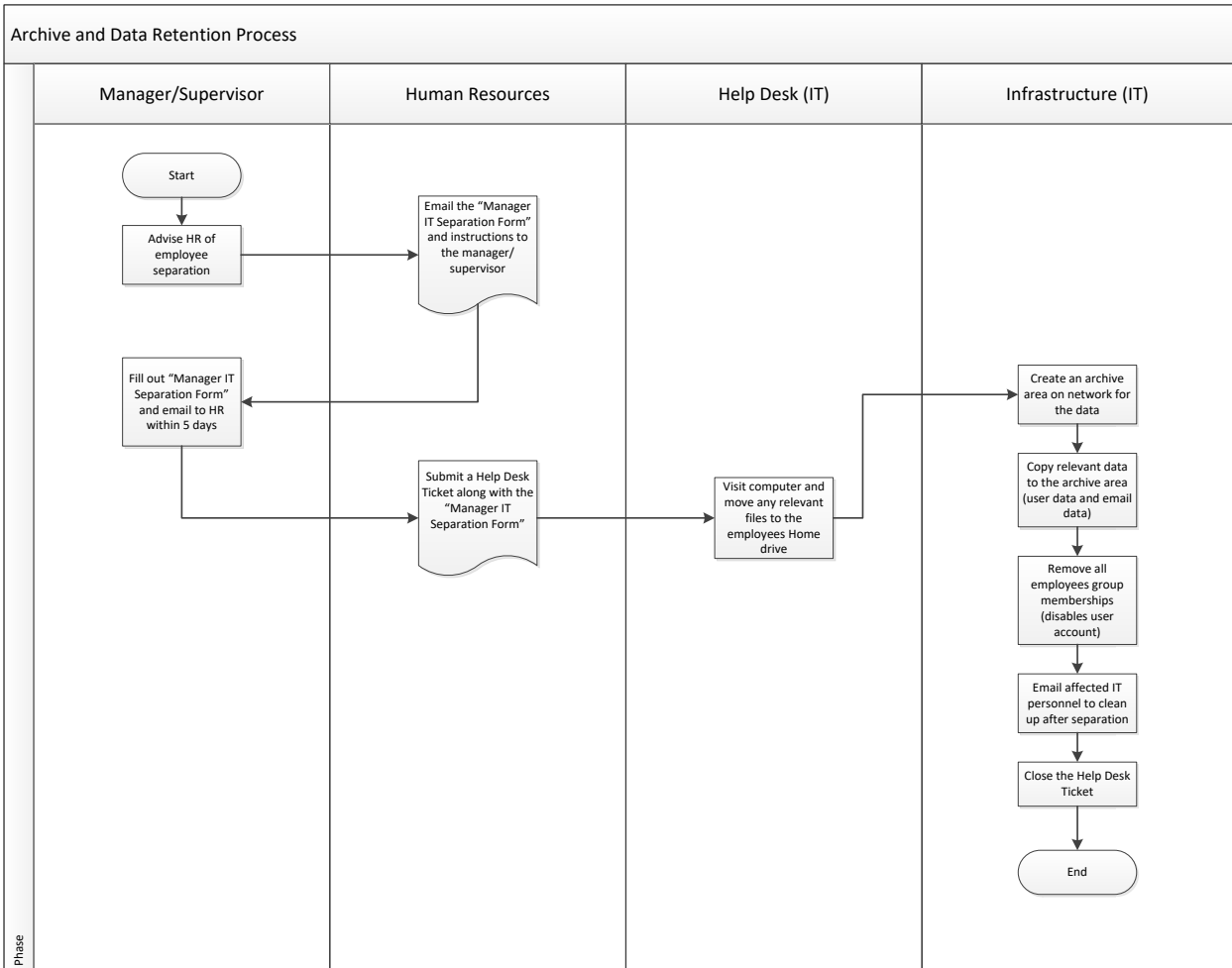
confidential manner. A Help Desk ticket will be created unless HR decides one should not be created.

- i. If an employee supervisor emails or calls IT with a separation request, the IT resource will re-direct the supervisor to the process and HR.
5. Help Desk staff will field the Help Desk ticket and visit the PC or laptop and move any relevant files to the employees Home directory. The Help Desk will contact the manager/supervisor to assist in the movement of files, if necessary.
6. The Infrastructure team fields the Help Desk ticket and performs the following tasks:
 - i. The assigned IT resource will:
 1. OneDrive for Business data remains as-is and is retained via retention policy, for a period of **forever**.
 2. **The mailbox is receiving a retention policy to ensure it is retained forever.**
 3. User data located on the network that is outside the user's network Home Directory stays in its original location and is backed up daily. If this data is not deleted it will continue to be backed up daily and will remain on the network forever, or until deleted. **Retention on daily backups is 42 days.**
 - ii. If requested, retrieve local data or grant access to the users mailbox for HR and (or) the employees supervisor.
 - iii. The assigned IT resources will remove all user group memberships
 - iv. The user account is disabled or it may be relocated in Active Directory for purposes of auto-response for a time frame requested by the supervisor. It will be kept active within IT.
 - v. Email all affected IT personnel to clean up separate accounts or access after separation.
 - vi. Infrastructure closes Help Desk ticket.
7. Asset stays in current location unless otherwise requested to remediate.
8. If asset is retained by Help Desk, the Help Desk:
 - i. Removes user info from the PC/laptop.
 - ii. Creates a new profile and reissues the PC/laptop.
 - iii. If requested, the data from an old system may be transferred to a new system.

New Process (Temporary Employees)

1. Department manager/supervisor separates the employee in Ultipro.
2. Department manager/supervisor submits a Help Desk ticket advising of the separation.
3. Help Desk fields the ticket, contacts the department manager/supervisor and fills out the attached "Manager IT Separation Form".
4. If needed, the Help Desk resource will work with the manager/supervisor to transfer any local files to a network share.
5. If needed, the Help Desk will assign the call to the Infrastructure group for any archiving of data.
6. The Infrastructure team fields the Help Desk ticket and performs the following tasks:
 - i. The assigned IT resource will:
 1. OneDrive for Business data remains as-is and is retained via retention policy, for a period of **forever**.
 2. **The mailbox is receiving a retention policy to ensure it is retained forever.**
 3. User data located on the network that is outside the user's network Home Directory stays in its original location and is backed up daily. If this data is not deleted it will continue to be backed up daily and will remain on the network forever, or until deleted. **Retention on daily backups is 42 days.**
 - ii. If requested, retrieve local data or grant access to the users mailbox for HR and (or) the employees supervisor.
 - iii. The assigned IT resources will remove all user group memberships.
 - iv. The user account is disabled or it may be relocated in Active Directory for purposes of auto-response for a time frame requested by the supervisor. It will be kept active within IT.
 - v. Email all affected IT personnel to clean up after separation.
 - vi. Infrastructure closes Help Desk ticket.
7. Asset stays in current location unless otherwise requested to remediate.
8. If asset is retained by Help Desk, the Help Desk:
 - i. Removes user info from the PC/laptop.
 - ii. Creates a new profile and reissues the PC/laptop.
 - iii. If requested, the data from an old system may be transferred to a new system.

3. Process Flowchart



4. Manager IT Separation Form

Manager IT Separation Form		
Employee	Employee Name:	
	Separation Date:	
	Manager:	
E-mail	What date should email access should be terminated?	
	Who should have access to current email folders?	
	Out of Office Message: Please edit	
***NOTE: Unless otherwise requested, the employee's email account will be discontinued in sixty (60)		
Files	Who should have access to the employee's network drive?	
	Who should have access to the employee's hard drive?	
Desk Phone	Voicemail Message: Please edit	
Laptop	Did the employee have a laptop?	
	<i>If YES, was it returned to IT?</i>	
	<i>If it was not returned to IT, who was it returned to?</i>	
***NOTE: Your department will continue to be charged for the laptop and air card unless otherwise		
Cell Phone (city issued)	Did the employee have a City issued cell phone?	
	<i>If YES, was it returned to IT?</i>	
	<i>If it was not returned to IT, who was it returned to?</i>	



INFORMATION TECHNOLOGY POLICY/PROCEDURE/PROCESS

Title:	709 – Scheduled and Unscheduled Systems Maintenance Procedure and Communications Plan	Document Number: 709
Effective:	July 13, 2022	
Supersedes:	August 31, 2020	
Approval:	Tom Shewchuk, IT Director ITLB	Page 1 of 3

1. Purpose

Define the protocol for addressing scheduled and unscheduled systems maintenance and how to communicate the status of systems that will/may not be available to our employees/users. Systems are defined as hardware and (or) software applications.

1.1. Rationale

- Routine systems maintenance is required to maintain the security, integrity, and availability of our systems. Because this maintenance can and may affect our users it is imperative that all systems maintenance schedules are communicated to our users.
- Proactively communicating scheduled maintenance will allow for more efficient problem resolution.
- Unanticipated issue(s) will occur from time-to-time. When this occurs it is crucial that the issues are addressed immediately by the right resources and the status of the issue(s) is communicated to all affected users until it is resolved.

2. Responsibilities

2.1. Scheduled Systems Maintenance

- Routine scheduled maintenance of the City's IT systems will be performed during the following defined ITSD Maintenance Windows. Discretion will be used by IT staff on the time maintenance will be performed in order to minimize any interruptions or the maintenance window will be suspended. If noticeable systems operations will be affected a communications to the affected

employees and the ITSD department must be sent out by a member of the infrastructure team. The “Help” account in Outlook will be used.

- **Maintenance Window 1 (IT Server Systems)** will be on Tuesdays from 5:15 PM to 11:59 PM. The availability of certain City systems will/may overlap the maintenance window.
- **Maintenance Window 2 (IT Server Systems)** will be on Sundays from 8:00 AM to 2:00 PM. The availability of certain City systems will/may overlap the maintenance Window.
- **Maintenance Window 3 (IT Server Systems)** will occur daily from 3:00 AM to 6:00 AM. The availability of certain City systems will/may overlap the maintenance window.
- **Maintenance Window 4 (PC Software Updates)** will be on every Wednesday from 7:00 PM to 11:59 PM. Users should save their work as they leave for the day, understanding that maintenance may necessitate computer reboots. The computer should be locked or logged off BUT remain powered on. There is a possibility that computers may need to be rebooted the following day if the computer was not powered on during the maintenance window.

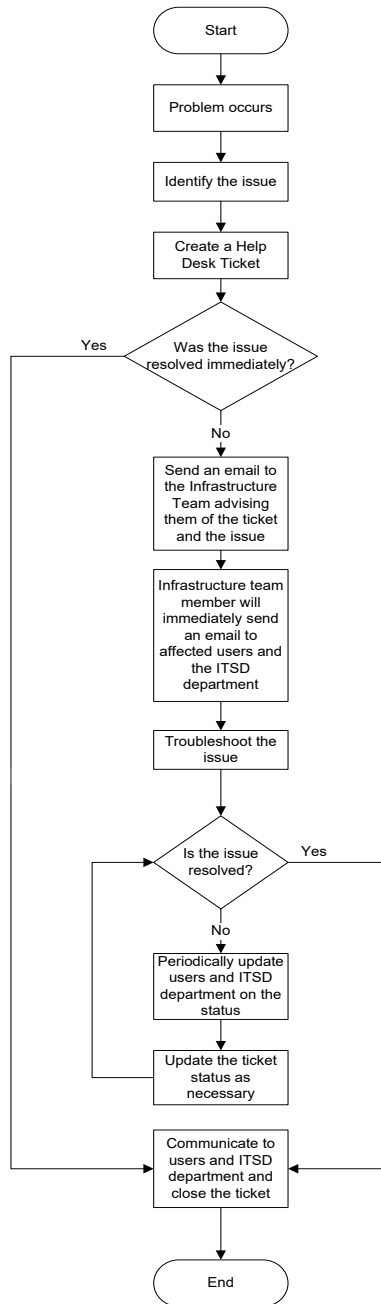
The maintenance window will be advertised to all city employees and no communications to our employees will be required if systems maintenance is routine and is performed during this window. Routine maintenance is primarily a proactive task applied to our systems on a regular basis in order to maintain our systems and software at a level recommended by our vendors.

2.2. Unscheduled Systems Maintenance

- Unanticipated problems will occur from time-to-time and our systems will become unavailable. If this happens, the affected employees/users must be advised immediately and updated on the status until the issue(s) is resolved. Below are the procedures to follow when this occurs:
 1. When a member of the ITSD team has determined there is a systems problem, identify the issue(s) and create a Help Desk ticket.
 2. If you are unable to resolve the issue, immediately send an email to O365InfrastructureTeam@a2gov.org advising them of the Help Desk ticket and issue.
 3. A member of the Infrastructure team will work with ITSD team member that reported the issue to understand the problem and immediately send an email to all affected users and the ITSD Department, using the “Help” account in Outlook, advising them of the problem along with clear and concise instructions.
 4. The ITSD team member and (or) the Infrastructure team member will troubleshoot the issue and the Infrastructure team member will update users and the ITSD Department at their discretion and based on the urgency, until the issue(s) is resolved.
 5. If determined the system needs to be taken down for maintenance the Infrastructure team member will advise the users and the ITSD Department on the date and time this will occur.

6. The Infrastructure Team member will update the Help Desk ticket with milestone information and at their discretion.

3. Unscheduled Systems Maintenance Process Flow





INFORMATION TECHNOLOGY POLICY/PROCEDURE/PROCESS

Title:	710 – On-Site Vendor/Guest Visitation	Policy Number:	710
Effective:	July 18, 2016		
Supersedes:	On-Site Vendor/Guest Visitation Policy - July 7, 2015		
Approval:	Tom Shewchuk, IT Director	Page	1 of 2

1. Purpose

Ensure secure access control to the IT Department Office, IT Infrastructure, Data Center, Network Operations (City Hall/Justice Center), Secondary Data Center Operations (Wheeler Field Ops Center) and all other City of Ann Arbor facilities.

1.1 Rationale

- Non-authorized personnel must be accompanied by City IT staff to mitigate security and safety risks.
- Michigan State Police (MSP) and the Federal Bureau of Investigation requires non-city personnel to either be escorted the entire duration of their visit to areas that possess Criminal Justice Information(CJI) or submit/pass a background check and take cyber security training administered by MSP.

1.2 Authorized Personnel:

- City of Ann Arbor staff
- Select City of Ann Arbor Field Operations Staff (Wheeler Field Operations Center only)
- Washtenaw County Staff
- Other personnel that have passed a City background check and has taken the MSP cyber security training

2. Responsibilities

The following responsibilities govern physical and network access controls for vendors and guests working within the City of Ann Arbor facilities and (or) having access to the City of Ann Arbor systems:

3. Notification of vendor/guest arrival:

The IT department staff will make every effort to advise appropriate IT personnel in advance of the arrival of a vendor or guest. At minimum the following information should be provided: Scope of work, arrival date/time, duration of the visit, the name of the vendor/guest and the company.

4. Vendor/Guest Sign-In/Sign-Out:

All vendors and/or guests must sign-in and sign-out using the visitor guest book located in the IT department and will be assigned an access control badge, if needed. The IT designee is responsible for making sure all vendors/guests sign-in and sign-out.

5. IT Designee Responsibilities:

- Assist and (or) accompany the vendor/guest during the entire duration of their visit regardless of the time of day.
- If the IT designee is not able to perform this task they must find and appropriate substitute.
- Upon arrival to the work area, verbal instructions will be provided to the visitor/guest on how to notify the IT designee when the visitor/guest is on-site.
- Direct supervision of vendors is required at all times.
- All vendors and visitors are required to meet with the IT designee before close of daily activities and provide IT designee and other responsible IT personnel with a brief update and synopsis of daily activities.
- If ID badges were assigned for completion of work, the badges must be returned to the IT designee when the vendor signs out.



INFORMATION TECHNOLOGY POLICY/PROCEDURE/PROCESS

Title:	711 – Remediation/Destruction of Digital Media	Policy Number: 711
Effective:	July 21, 2016	
Supersedes:	n/a	
Approval:	Tom Shewchuk, IT Director	Page 1 of 2

1.0 Purpose

When digital media is delivered or acquired by the Information Technology department, it must be remediated, destroyed and (or) discarded in a responsible and secure manner. The following procedures will define media and the methods in which it will remediated and (or) destroyed.

1.1 Rationale

- As a cyber security best practice, media at rest or no media no longer needed, especially sensitive information such as Criminal Justice Information (CJI), must be remediated.
- Michigan State Police (MSP) and the Federal Bureau of Investigation requires require the City of Ann Arbor Police department to have a digital media remediation policy for any media possessing CJI.

1.2 Digital Media Types (but not limited to):

- Hard/SSD drives
- CD/DVD's
- Flash media
- Tapes
- Floppy Disks
- Tablet and Cell Phones with non-removable storage
- Any other digital media

2.0 Responsibilities

The following procedures will be followed when the IT department receives digital media that is no longer needed:

1. When digital media is brought to IT and (or) acquired by IT, a Help Desk ticket will be created.
2. The Help Desk ticket will be assigned to the appropriate IT Team Member.
3. The Team member will proceed as follows:
 - a. Hard/SSD Drives will be destroyed using the Data Destroyer MVHD-1C hard drive shredder.
 - b. All floppy disks, CD/DVD's and floppy disks will be shredded using the Fellows C225C cross cutting shredding machine in the IT department copy room.
 - c. The memory chip on all flash media will be physically destroyed and properly disposed of.
 - d. All Tablets and Cell Phones will be reset to factory default then disposed of properly or remediated.



INFORMATION TECHNOLOGY POLICY/PROCEDURE/PROCESS

Title:	712 – Onboarding and Termination of Users' Computer Access	Policy Number: 712
Effective:	April 13, 2022	
Supersedes:	March 1, 2022	
Approval:	Tom Shewchuk, IT Director	Page 1 of 2

Purpose

Ensures secure practices and standard methodology for establishment of network user access for new hires. Similarly standardizes termination of access upon separation of employment, while maintaining security and preventing unauthorized access to our computer systems.

Rationale

- Access to computer systems is required for many job roles throughout the City of Ann Arbor
- A standard, uniform process needs to be applied to establishment of computer access. Access cannot be granted until all prerequisites have been completed.
- Access to computer systems must be terminated once employment with the City of Ann Arbor has ended (due to voluntary or involuntary separation, retirement, or death).

Onboarding Responsibilities

Information Technology is not to grant computer access until so authorized by Human Resources.

Human Resources notifies Information Technology of authorization to grant computer access via IT's helpdesk ticket system. The new employee's supervisor should provide HR all available information with regards to computer access needed.

IT routes the helpdesk ticket to the Infrastructure Team. A user account is created, and appropriate access and rights are granted.

Termination Responsibilities

Authorization to revoke computer access to an employee can come from a variety of sources depending on the status of the employee:

- Regular Employees: Authorization to revoke access should come from Human Resources. Revocation authorization will also be accepted by IT from any appropriate manager or supervisor of the employee in question. If notice does not come from HR, IT will notify HR.
- Temporary Employees (or other non-regular employees such as contractors): Authorization to revoke access should come from the employee's supervisor. HR is not involved in the separation process of temp employees.

Authorization to revoke access should be received by IT in the form of a help desk ticket. If there is time sensitivity to the revocation of access, other forms of communication are acceptable (phone call, email, in person visit, Teams message) and need to be documented after the fact via helpdesk ticket.

IT routes the helpdesk ticket to the Infrastructure Team. Access is revoked via disabling of Active Directory user account and badge access at the appropriate time (immediately, if so requested, or at a scheduled date and time that corresponds to the employee's final departure).

At a later date, Infrastructure Team member performs additional activities to complete termination process.

- User's OneDrive for Business data is preserved via M365 retention policies
- Data from Exchange mailbox is preserved via litigation hold as licensing is removed. Mail can be forwarded to other recipients as requested or access to the mailbox can be granted as requested.
- Helpdesk contacts separated employee's supervisor and inquires if any data retrieval should be performed from the employee's desktop or laptop. Any data identified will be provided to Infrastructure Team to copy OneDrive area for retention
- Active Directory user account is held in a disabled state for 13 months. After 13 months, ID is permanently deleted.
- Infrastructure Team notifies other members of Information Technology to revoke other access
 - Jim Clare: local SQL server accounts
 - Dave Wilburn: Cityworks and Geocortex access
 - Kyle Spade: LOGOS access
 - Anna Simmons and/or Scott Harrod: TRAKiT access
 - Jason McKinley: disables all access within CJIS applications for Police and City Attorney's Office
 - Jena Miras: disables all access within CJIS applications for 15th District Court

Termination Audit Policy

Infrastructure Team conducts audits of Active Directory to ensure user access has been revoked for separated employees as follows:

- On a monthly basis, reports are run from UltiPro.
 - Any job changes are recorded in Active Directory as appropriate
 - Separation listings are reviewed. Any terminations found that have not been processed by the Termination Responsibilities in this document are followed up upon and access is revoked as appropriate.
- On a quarterly basis
 - A report is run from UltiPro to review all users within Active Directory. Any terminations shown in UltiPro that are not reflected in Active Directory are followed up upon and access is revoked as appropriate.
 - A report is run from Active Directory to review network user ID activity. Any user IDs that have been inactive for 70 or more days are handled as follows:
 - The user ID is disabled
 - The account is placed into a hold state for 13 months
 - If the user ID is still disabled after 13 months, the account is disabled, and data is archived as follows:
 - OneDrive for Business data is preserved via M365 retention policies. Data from Exchange mailbox is preserved via litigation hold as licensing is removed
 - Helpdesk contacts separated employee's supervisor and inquires if any data retrieval should be performed from the employee's desktop or laptop. Any data identified will be provided to Infrastructure Team to copy to OneDrive preservation hold area.
 - Application level permissions are reviewed on a quarterly basis. As these applications are accessible on network only, they cannot be accessed by staff with the Active Directory account disabled at separation. Account access is managed as follows:
 - Dave Wilburn
 - Mainsaver
 - ITPipes
 - Paradigm
 - Roadsoft
 - Gas Boy/OrPak Fuel System
 - MERL
 - Cityworks
 - Geocortex
 - Field Manager
 - Digsmart
 - CalAmp (AVL) / iOn
 - Kyle Spade
 - LOGOS
 - Anna Simmons or Scott Harrod:
 - TRAKiT
 - Energov
 - Jason McKinley
 - Oversees CJIS/LEIN applications which are also administered within the service units as appropriate



INFORMATION TECHNOLOGY POLICY/PROCEDURE/PROCESS

Title:	713 – Power Testing for Data Centers	Policy Number:	713
Effective:	August 24, 2016		
Supersedes:	N/A		
Approval:	Tom Shewchuk, IT Director	Page	1 of 2

1.0 Purpose

Document standards for power protection for computing equipment in City of Ann Arbor data centers (located in the Justice Center and Wheeler Service Center).

2.0 Standards

Information Technology relies on multiple methods to keep power running reliably to protect key networking and server computing equipment.

The data center located in the Justice Center building utilizes both a Liebert NX 120kva UPS and Enersys cabinet containing 2 x 40 battery strings. This 3 phase unit distributes power to each of the equipment racks where each of the devices located in these racks have their power distributed across multiple phases. By requiring dual power supplies in each device and connecting each of these power supplies to separate power phases, we've achieved the highest redundancy possible.

The data center located in the Wheeler Service Center datacenter building utilizes both a Liebert NX 80kva UPS and Enersys cabinet containing a 40 battery string. This unit and all connected equipment follow the same guidelines as the Justice Center data center.

Each of these units and their associated battery strings have maintenance/inspections performed twice yearly.

In addition, we are relying on the City's generators and power provided by Facilities. The generators at both facilities are exercised weekly. Facilities tests each facility twice yearly. One of these tests is a load test, in which the generators are activated and feed power into a bank of resistors to see how they handle a load draw.



INFORMATION TECHNOLOGY POLICY/PROCEDURE/PROCESS

Policy Title:	714 - Email Signature Policy	Policy Number:	714
Effective:	August 28, 2019		
Supersedes:	N/A		
Approval:	Howard S. Lazarus, City Administrator Tom Shewchuk, IT Director	Page	1 of 3

1. Purpose

The purpose of this policy is to establish a standard email signature format for all persons with an assigned City of Ann Arbor email.

2. Rationale

Email is an important form of communication, both internally and externally. When we communicate electronically, we are acting as representatives of our respective departments and the City of Ann Arbor. The goal of a standard email signature format is to:

- Reflect the professionalism of the City of Ann Arbor.
- Be respectful and thoughtful.
- Be consistent and uniform among all authorized email users.

3. Roles and Responsibilities

All persons with an authorized City of Ann Arbor email account must read, understand, and comply with this policy.

4. Implementation

All persons using the City of Ann Arbor email system must have an email signature and must use the following format and elements on all City Outlook email signatures (including use of email on mobile devices).

5. Standard Email Signature Format

Required

- ✓ Name
- ✓ Title
- ✓ City Name
- ✓ Location
- ✓ City, State, Zip
- ✓ Phone Number (can be the main City number)
- ✓ Employee email address
- ✓ City web address

Optional

- ✓ Direct Phone Number (DID) (Required for internal email, optional for external, but not required if the device sending the email cannot make a distinction between the two)
- ✓ Fax Number

Font and Size Requirements:

- ✓ Font: Calibri, Times New Roman, Verdana or Arial
- ✓ Sizes: 8, 9, 10, 11, or 12

The following items are not allowed:

- ✓ No credos, mottos, quotations, or individual statements
- ✓ No borders or backgrounds
- ✓ No decorative or script fonts
- ✓ No unapproved City logos

**Sample Format (feel free to cut and paste and modify to your signature):*

Joe Smithfield, Engineer

City of Ann Arbor | Guy C. Larcom City Hall | 301 E. Huron, 3rd Floor · Ann Arbor · MI · 48104
734.794.0000 (O) · 734.794.0000 (F) | Internal Extension 00000
jsmithfield@a2gov.org | www.a2gov.org

6. Optional Signature Statements/Notice/Employee Photo

Each supervisor and manager may determine whether employees in that specific work area are required to add the following statements below their email signature. If required to do so, please cut and paste. Other approved City logos, graphics, or statements may be used with supervisor approval.

Confidentiality Notice (cut & paste verbatim):

CONFIDENTIALITY NOTICE: This e-mail, and any attachments, is for the sole use of the intended recipient(s) and may contain information that is confidential and protected from disclosure under the law. Any unauthorized review, use, disclosure, or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail, and delete/destroy all copies of the original message and attachments.
Thank you.

Environmental statement (cut & paste verbatim):



Think Green! Please don't print this e-mail unless absolutely necessary.

Safety statement (cut & paste verbatim):

A2 Be Safe. Everywhere. Everyone. Every day.
a2gov.org/A2BeSafe

OR



EVERYWHERE • EVERYONE • EVERY DAY.
a2gov.org/A2BeSafe

Employee picture (optional):

An employee picture must be an actual photo of an employee or an original graphical depiction meant to resemble the employee and must have a neutral background and a professional appearance. An employee picture cannot contain writing and cannot be a recognizable cartoon character (for example, Mickey Mouse). Supervisors and managers have the right to ask an employee to remove a picture if it does not comply with this policy.



INFORMATION TECHNOLOGY POLICY/PROCEDURE/PROCESS

Title:	715 – Media Protection Policy	Policy Number:	715
Effective:	February 25, 2019		
Supersedes:	N/A		
Approval:	Tom Shewchuk, IT Director	Page	1 of 4

1.0 Purpose

This policy ensures the protection of the Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules. The local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

2.0 Scope

The scope of this policy applies to any electronic or physical media containing MI/FBI Criminal Justice Information (CJI) while being stored, accessed or physically moved from a secure location from City of Ann Arbor LEIN agencies (15th District Court, Ann Arbor Police, City Attorney's Office). This policy applies to any authorized person who accesses, stores, and / or transports electronic or physical media. Transporting CJI outside the agency's assigned physically secure area must be monitored and controlled.

Authorized City of Ann Arbor personnel shall protect and control electronic and physical CJI while at rest and in transit. The City of Ann Arbor will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the City of Ann Arbor Local Agency Security Officer (LASO)/Terminal Agency Coordinator (TAC). Procedures shall be defined for securely handling, transporting and storing media.

3.0 Media Storage and Access

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

“Physical media” includes printed documents and imagery that contain CJI. To protect CJI, the City of Ann Arbor personnel shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.
2. Restrict access to electronic and physical media to authorized individuals.
3. Ensure that only authorized users remove printed or digital media from the CJI.
4. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures. (See Policy 711 Remediation/Destruction of Digital Media)
5. Not use personally owned information system to access, process, store, or transmit CJI unless the City of Ann Arbor has established and documented the specific terms and conditions for personally owned information system usage.
6. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
7. Store all hardcopy CJI printouts maintained by the City of Ann Arbor in a secure area accessible to only those employees whose job function requires them to handle such documents.
8. Safeguard all CJI by the City of Ann Arbor against possible misuse by complying with the all relevant policies.
9. Take appropriate action when in possession of CJI while not in a secure area:
 - a. CJI must not leave the employee’s immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
 - b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.
 - i. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.
 - ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.
10. Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need-to-know basis.
11. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJI.

4.0 Media Transport

Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. “Electronic media” means electronic storage media including memory devices in laptops

and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Dissemination to another agency is authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or
2. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

The City of Ann Arbor personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.
2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

The City of Ann Arbor personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.
2. Limiting the collection, disclosure, sharing and use of CJI.
3. Following the least privilege and role based rules for allowing access. Limit access to CJI to only those people or roles that require access.
4. Securing hand carried confidential electronic and paper documents by:
 - a. Storing CJI in a locked briefcase or lockbox.
 - b. Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.
 - c. For hard copy printouts or CJI documents:
 - i. Package hard copy printouts in such a way as to not have any CJI information viewable.
 - ii. That are mailed or shipped, agency must document procedures and only release to authorized individuals. **DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL.** Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.
5. Not taking CJI home or when traveling unless authorized by City of Ann Arbor LASO. When disposing confidential documents, use a cross-cut shredder.

5.0 Electronic Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures. For end of life media policy, refer to Policy 711 Remediation/Destruction of Digital Media.

6.0 Breach Notification and Incident Reporting

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The CSA ISO Computer Security Incident Response Capability Reporting Form CJIS.016 can be accessed and completed at www.michigan.gov/lein under the Sample Documentation button. The completed form can be submitted via email, directly from the form.

7.0 Roles and Responsibilities

If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. City of Ann Arbor personnel shall notify his/her supervisor or LASO, and an incident-report form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident.
2. The supervisor will communicate the situation to the LASO to notify of the loss or disclosure of CJI records.
3. The LASO will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.
4. The CSA ISO will:
 - a. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.
 - b. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
 - c. Act as a single POC for their jurisdictional area for requesting incident response assistance.

8.0 Penalties

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.



INFORMATION TECHNOLOGY POLICY/PROCEDURE/PROCESS

Title:	716 – Artificial Intelligence (AI) Usage Policy	Policy Number: 716
Effective:	August 5, 2025	
Supersedes:	N/A	
Approval:	Joshua Baron, IT Director	Page 1 of 5

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 to all employees, contractors, visitors, vendors, City volunteers, unpaid interns, and third-party vendors who may use AI Tools while handling city data ("Users"), including confidential or sensitive information. All users of City electronic communication systems are expected to comply with this policy as a condition of continued employment and/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 establish guidelines and best practices for using Artificial Intelligence (AI) Tools, ensuring the protection of the City's confidential and sensitive information.

The key objectives of this policy include:

- Provide guidance that is clear, easy to follow, and supports decision-making for the staff (full-time, part-time), interns, consultants, contractors, partners, and volunteers who may be purchasing, configuring, developing, operating, or maintaining the City's AI Tools or leveraging AI Tools to provide services to the City.

- Ensure that when using AI Tools, the City or those operating on its behalf, adhere to the guiding principles that represent values with regards to how AI Tools are used, purchased, configured, developed, operated, or maintained.
- Define prohibited uses of AI Tools.

3. Definitions

- **Confidential Information:** Any non-public information that could cause harm to the City or its employees if disclosed, including but not limited to all Personally Identifiable Information, and information protected under HIPAA or the CJIS Security Policy, or data governed by PCI DSS, defined below.
- **Artificial Intelligence (AI) Tools:** AI Tools encompass any software, application, or system leveraging technologies such as machine learning, natural language processing, or other forms of artificial intelligence. These tools may include, but are not limited to:
 - Generative AI: Platforms like ChatGPT, Google Gemini, DALL·E, and MidJourney that create text, images, audio, or other content.
 - Predictive Analytics Tools: Applications such as IBM Watson or SAS Analytics that forecast outcomes or trends based on data.
 - Recommendation Systems: Systems like Google Cloud Recommendations AI or Amazon Personalize that provide tailored suggestions.
 - Decision Support Systems: Tools like Microsoft Azure Cognitive Services or Salesforce Einstein that assist in decision-making by analyzing data and patterns.
 - This list is not exhaustive, as the field of AI is rapidly evolving. If you have questions about whether a particular tool or application falls under this category, or if you are unsure about its appropriate use, please seek clarification from the IT Department.
- **Payment Card Industry Data Security Standard (PCI DSS):** a set of requirements that ensure the security of credit card information.
- **Personally Identifiable Information (PII):** any information that can be used to identify a person, either directly or indirectly:
 - Directly: Includes a person's name, address, social security number, telephone number, or email address
 - Indirectly: Includes a combination of other data elements, such as gender, race, birth date, or geographic indicator

- **Health Insurance Portability and Accountability Act (HIPAA):** the statute that controls and protects the confidentiality of any individually identifiable health information, such as medical records, treatment details, or payment information.
- **Criminal Justice Information Services (CJIS):** the system which contains sensitive information, such as criminal justice records, fingerprints, or investigative reports, that is protected under the U.S. Department of Justice Criminal Justice Information Services (CJIS) Security Policy¹

4. Acceptable Use of AI Tools

- AI Tools must only be used for approved work-related tasks.
- Users must not input, upload, or share any confidential or sensitive information, including but not limited to PII, into AI Tools unless:
 - The tool has been vetted by the City's IT team.
 - The AI provider has been contractually obligated to maintain confidentiality and data security standards.
- AI Tools should not be relied upon for decision-making in critical business processes without human oversight.
- Users should be aware of the risk of mistakes, errors, and inaccurate outputs when using AI Tools. Output should be validated by other sources whenever possible. Additionally, human review and proofreading is crucial for all AI-generated communications to ensure accuracy and clarity.

5. Prohibited Use

- Under no circumstances should Users use external or consumer-grade AI Tools (e.g., free or public AI systems) to process Confidential Information, including but not limited to data governed by PCI DSS, HIPAA, CJIS standards, or personally identifiable information (PII) as defined in Section 3, 'Definitions'.
- Users must not:
 - Use AI Tools to generate content that includes any form of confidential City data unless explicitly authorized by the City Administrator or their designated representative.
 - Copy or transfer confidential data into AI platforms that have not been approved by the City's IT team.

¹ https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

- Share outputs generated by AI Tools that involve sensitive information unless explicitly authorized by the City Administrator or their designated representative.

6. Data Handling

- Users should ensure that any data shared with AI Tools is anonymized or redacted to remove identifying or sensitive details.
- Users should ensure that any AI Tools used to handle sensitive data have secure connections (e.g., the website URL should begin with 'https://').

7. Monitoring and Compliance

- The City will periodically monitor the use of AI Tools to ensure compliance with this policy.
- Any unauthorized use of AI Tools to handle confidential data will result in disciplinary action, up to and including termination.

8. Training and Awareness

- All employees, volunteers, and unpaid interns must undergo regular training on the appropriate use of AI Tools and the importance of data security.
- Users should be made aware of the risks of mishandling confidential information when using AI.

9. Reporting and Incident Management

- Employees, volunteers and unpaid interns must immediately report any accidental disclosure of confidential data to unauthorized AI systems.
- The City will thoroughly investigate all incidents of non-compliance involving the use of AI Tools and potential breaches of confidentiality. Investigations will be conducted under the joint oversight of the **IT Department**, the **City Attorney's Office**, and the **Human Resources Department**, as appropriate.

Upon identification or reporting of a potential incident:

1. The **IT Department** will assess the technical aspects of the breach, including identifying the tool used, the scope of the data involved, and the potential impact on City operations or constituents.
2. The **City Attorney's Office** will evaluate compliance with applicable laws, regulations, and City policies, ensuring that the City's liability and legal exposure are properly addressed.

3. The **Human Resources Department** will manage employee-related aspects of the investigation, ensuring due process and adherence to City employment policies.

Corrective actions may include, but are not limited to:

- Technical measures to mitigate further risks (e.g., tool access restrictions).
- Legal actions to protect the City's interests.
- Employee training, disciplinary action, or termination, depending on the severity of the incident.

Employees, City volunteers and unpaid interns are required to immediately report any suspected or actual breaches of this policy to their unit manager, who will promptly escalate the report to the IT Director. All reports will be treated with urgency and confidentiality, consistent with applicable laws and regulations.

10. Attribution and Plagiarism

- Users must not present AI-generated content as entirely original if it substantially contributes to an official City communication, report, or policy.
- Use of AI to draft content must be transparent and attributed where appropriate.
- Plagiarism—including copying from AI Tools without acknowledgment—is prohibited.
- When appropriate, annotate or footnote the use of AI to support transparency and public trust.

11. Recording and Meeting Capture Guidelines

- Recording of online meetings is strictly prohibited in all cases, except for those instances outlined below.
 - The following meetings may be recorded and/or transcribed. All meeting attendees must be notified at the beginning of the meeting that the meeting is being recorded. Public meetings required to be recorded by law
 - Training intended for redistribution
 - Accessibility accommodations
- All recordings and transcriptions must comply with retention schedules and data security protocols.

- Unauthorized recordings may result in disciplinary action.
- The use of “Live Captioning” is permitted. However, any form of recording the meeting while using live captioning, including screen shots of the meeting in progress, is prohibited.

12. Policy Updates

This policy will be reviewed and updated regularly to account for advancements in AI technology and changes in data security practices.

GLOSSARY

Access

There are two types of access – **Physical** and **Logical**.

1. **Physical Access.** The process of obtaining use of a computer system, - for example by sitting down at a keyboard, - or being able to enter specific area(s) of the organization where the main computer systems are located.
2. **Logical Access.** The process of being able to enter, modify, delete, or inspect, records and data held on a computer system by means of providing a User ID and password.

Access Control

A principle of limiting access to computerized information to authorized individuals or information systems (applications, systems, etc.). It refers to the rules and deployment mechanisms that control access to information systems, and physical access to premises.

Access Point (AP):

A hardware device that connects wireless clients to the City network. Usually mounted on ceilings or high walls.

Access Rights

The powers granted to users to create, change, delete, or view data and files within a system.

Account

A mechanism used to control access to information systems and assign access rights (e.g. a User ID). Before resources on systems are utilized, accounts must be created for users or processes.

Accountability

A principle that enables all actions to be traced back to an individual who may be then be held responsible for their actions.

Anti-Virus Program

Software designed to detect, and potentially eliminate, computer viruses, as well as repairing or quarantining files which have already been infected by virus activity.

Appliance

Specialized equipment that is designed for ease of installation and maintenance. Appliances typically have their hardware and software bundled and pre-installed. An appliance is intended to connect into an existing environment and begin working almost immediately, with little configuration. Appliances typically contain vendor-supplied or embedded operating systems and are vendor supported.

Application

A software program or group of software programs used to perform specific business functions for multiple users, or in some cases other software programs.

Application Architecture

The fundamental organization (i.e. architecture) of an information system (i.e. application). Defines process, data, and technology components and their relationships.

Archive

An area of data storage set aside for non-current (old or historical) records in which the information can be retained under a restricted access regime until no longer required by law or organization record retention policies.

Archiving

The process of moving non-current records to the Archives.

Authentication:

A method of proving that the identification (usually a User ID) presented to an information system is valid. This is typically a password. There are three types of authentication:

Type 1. Something only the user knows such as a password, response to a challenge question, etc.

Type 2. Something the user has, such as a SecurID token, smart card, etc.

Type 3. Something the user is (biometrics), such as fingerprints.

Authentication systems can use any single method, a combination of any two methods (two-factor authentication) or use all three methods (three-factor authentication). Note: using two authentication methods of the same type (e.g. using two passwords to authenticate to a computer) is not two-factor authentication.

Authorization:

1) The resources and access rights granted to a user, process, system, etc. after the person/process/etc. is authenticated.

2) The process whereby a person approves a specific event or action.

Availability

The assurance that information remains accessible when required. Availability is a security goal and one of the elements of the Confidentiality, Integrity, and Availability (CIA) classification model. It relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities. If a mission-critical IT system is unavailable to its users, the organization's mission may be affected.

Backup

The process whereby copies of computer files are made in order to allow recreation of the original, should the need arise. A backup is a spare copy of a file, system, or other information resource for use in the event of failure or loss of the original.

Batch

The execution of a series of programs on a computer without human interaction.

Batch User ID

An identification code (User ID) used to perform a batch (a sequence of commands or a group of tasks run in non-interactive background mode) processing.

Business Case

The Business Case forms the foundation for any proposed venture or project. It establishes (in commercial / business terms) the need, justification and proposed alternatives to resolving a business issue or meeting a strategic objective.

Business Continuity Plan (BCP)

A predefined set of actions that provide the ability to assess the impact of an event, activate appropriate actions, recover critical business operations, and restore normal business processes. This is a plan to ensure that the essential business functions of the organization are able to continue (or re-start) in the event of unforeseen circumstances, normally a disaster of some sort. However, BCP is not to be confused with Disaster Recovery Planning, which is focused upon crisis management.

Having dealt with the immediate crisis: securing the health and safety of people and preventing further spread or continuation of the crisis (e.g. a fire), the Disaster Recovery Plan will hand over to those responsible for executing the Business Continuity Plan. The BCP will identify the critical people (roles / functions), information, systems and other infrastructure, e.g. telephones, which are required to enable the business to operate. The BCP will lay out a detailed plan that, if called upon, should be executed to assure minimum additional disruption.

Business Requirements

The needs of the business processes that must be addressed by either a manual or computerized system. It is critical that the business requirements be clearly defined and documented.

Capacity Planning

Capacity Planning is the determination of the overall size, performance and resilience of a computer or system. The detailed components of a Capacity Planning initiative will vary, depending upon the proposed usage of the system, but the following should always be considered:

- The expected storage capacity of the system and the amount of data retrieved, created and stored within a given cycle.
- The number of on line processes and the estimated likely contention.
- The required performance and response required from both the system and the network i.e. the end-to-end performance.
- The level of resilience required and the planned cycle of usage – peaks, troughs and average.
- The impact of security measures e.g. encryption and decryption of all data.

Change Control

An internal control procedure by which only authorized amendments are made to the organization's software, hardware, network access privileges, or business process etc.

Commercial software

Software for which the City receives authorization through receipt of a license for the "right to use" the product from the originating person, organization, or City. In general, the City pays a fee for the license, although this is not always a requirement. Commercial software is protected by copyright. The owner of a copyright for software, usually the developer, has the right to prohibit other people from making copies, except as stated in a license or in copyright law.

Commission

The commissioning of a (computer) system is the point when it is put into live, operational, and active service.

City-owned software

Software written by City employees or by persons under contract to the City whereby the City acquires copyrights to the software. This software must not contain any commercial or third-party software unless permission for use has been granted by the copyright owners of the software.

Computer:

A programmable device that performs mathematical calculations and logical operations, especially one that can process, store and retrieve large amounts of data very quickly. A computer runs an operating system (such as Microsoft Windows), can have peripheral hardware (such as a monitor, mouse, keyboard, printer, etc), and runs application programs (such as word processing applications, web browsers, mobile apps, etc.). This definition includes but is not limited to desktops, laptops, and mobile devices.

Computer Systems:

One or more computers, with associated peripheral hardware, with one or more operating systems, running one or more application programs, designed to provide a service to users. Includes desktops, laptops, and mobile devices.

Computer Virus

Pieces of programming code which have been purposely written to inflict an unexpected result upon a computer system.

Consultant

A user who works directly in the City under a contract between the City and the user, or the user's employer.

Contract Services

A user who works directly in the City under a contract between the City and the user's employer.

Controls

Controls are automatic or manual countermeasures intended to prevent, detect, or correct errors, omissions, accidents, or deliberate acts that could affect the computer's accuracy, integrity, availability, or security. Unless otherwise stated controls are mandatory. Controls meet broad policy objectives. For example, a policy might require that sensitive data be protected on removable media (Portable media, CD-ROM, etc.). The control would be to encrypt the data on removable media.

Core

Core technology represents the strategic infrastructure direction of the City. All strategic investments should be made according to the core technology standards. Core components are replicated and supported throughout the City.

Core Declining

Core-declining technology represents technology that previously was core, but which does not represent the present strategic direction for City technology investments. It may be broadly deployed and may be required for the processing of critical systems. The expectation is that core-declining technology will gradually be replaced by core technology.

Data

- Computerized information.
- Information processed by an information system and owned by the originator of the information.
- The smallest discrete unit of information organized in a database that needs to be combined with other data and processes in order for it to be understood.

Data does not necessarily represent a record because it may or may not have been created in the conduct of business, and preserved as evidence of a decision or action.

Data Center

A room or building used primarily to house computer equipment, power, and air conditioning supply areas. This equipment is usually located in a special room because of the need for physical security, temperature control, power redundancy, and fire protection.

Data Owner

The person who creates, or initiates the creation or storage of the information, is the initial owner. In an organization, possibly with divisions, departments and sections, the owner becomes the unit itself with the person responsible, being the designated 'custodian' of that data.

Database

A collection of files, tables, forms, reports, etc., held on a computer system that have a predictable relationship with each other for indexing, updating, and retrieval purposes.

Decryption

The process by which encrypted data is restored to its original form in order to be understood/usable by another computer or person.

Desktop

Verbal shorthand for Desktop Personal Computer, normally used to differentiate such a system from a 'Laptop' or portable PC.

Digital Certificate

A digital certificate is the electronic version of an ID card that establishes the user's credentials and can be used to authenticate connections over the Internet or Intranet.

Digital Signature:

A process applied to an electronic communication that verifies the sender's identity and validates that the message was not forged or modified.

Distributed Processing

Spreading the organization's computer processing load between two or more computers, often in geographically separate locations.

Downtime

The amount of time a system is down in a given period. This will include crashes and system problems as well as scheduled maintenance work.

Electronic Data

Data stored on electronic storage media.

Electronic Communications

Computer-facilitated communications including but not limited to: email, instant messaging (IM), and text messaging.

Electronic Mail (Email)

A method of exchanging digital messages from an author to one or more recipients via an electronically transmitted message. This message is stored on and retrieved from an organization's server.

Electronic Storage Media

Storage devices in computers or any removable storage medium which is capable of storing data in an electronic format, such as a computer hard drive, CD, DVD, USB drive, digital memory card, personal digital assistant (PDA), personal media player, cell phone or other similar device.

Emerging technology

Emerging technology represents technology that the City is considering for eventual deployment into core technology or into a peripheral role. Emerging technology can represent a unique new service for the infrastructure or the same service, but with a significantly new product or standard.

Encryption

The process of coding information so that its content is not understandable to anyone who obtains the information. To read the information, an algorithm is required to restore the information to its original form. Information also may be one-way encrypted so that it is not possible to restore the information to its original form. One-way encryption typically is used to protect passwords while they are stored on a computer system.

Enterprise Network

Term meant to encompass all City controlled networks.

End-User

The person who actually uses the hardware or software that has been developed for a specific task.

Event

A situation or set of circumstances that may lead to the loss, prevention or reduced functionality of a business process.

External Email

Email sent, or received from, outside the City Networks.

External Facing

Applications and websites that are accessed by external users (including but not limited to suppliers, dealers, consumers, etc.) and all City web systems (developed internally or externally) that reside on the extranet or Internet.

Firmware

Software or code stored permanently or semi-permanently on a memory chip.

Graphical User Interface Guidelines (GUI)

A type of user interface that allows users to interact with electronic devices with images rather than text commands.

Hard copy

A copy on paper, as opposed to any other storage medium.

Hardware Physical equipment:

Computers, screens, keyboards, mice, printers, scanners, network routers, switches, racking, disk drives, portable drives, etc.

Help Desk

ITSU Staff who are responsible for assisting other staff members in the use of computer systems, resolving problems which may arise, and routing failures or advanced issues to the appropriate IT personnel.

Host

An information system contacted through a network by subordinate computers (PCs, terminals, etc) for processing or information. An endpoint device.

Independent Contractor

User works directly in the City under a contract between the City and the user.

Information Management

The coordinated management of a City's information-based resources, including its information holdings and investments in technology.

Information Systems

Information Systems (also referred to as “systems”) – The computer systems and information sources used by an organization to support its day-to-day operations. Examples include applications, infrastructure, tools, appliances and web sites.

Information Systems Owner

The operational activity (stakeholder) whose business process is supported by the information system. The stakeholder is the committee or individual who controls the maintenance and development budget for the information system. If an information system has more than one owner, a primary owner or a steering group with representatives from all owners, should be designated. The owner of the information system may also assess the risk and identify the security and control requirements that must be met to protect the information system.

Infrastructure

Hardware devices and/or software components which provide the underlying foundation or framework that enables and supports applications. Functions that infrastructure provide include, but are not limited to, operating system functions, backup and recovery, communication & messaging, networking, database management, scheduling, user access security, and physical security. Examples of Infrastructure include, but are not limited to: Windows, Linux, Virtual Machines (VMs), SQL, scheduling software, badge reader software, etc.

Infrastructure Control Review (ICR)

A process to ensure that effective controls are designed and implemented for infrastructure, appliances and similar systems.

Integrity

The assurance that information is accurate and has not been improperly modified, either intentionally or unintentionally. Integrity is a security goal and one of the elements of the CIA classification model. It relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations. Integrity is lost if unauthorized changes are made to the data or IT application by either intentional or accidental acts. If the loss of application or data integrity is not corrected, continued use of the contaminated application or corrupted data could result in inaccuracy, fraud, or erroneous decisions.

Internet (also Public Internet)

A publicly accessible Wide Area Network that can be employed for communication between computers. Some features of the Internet include Search Engines, Social Networking, Bulletin Boards, On-Line services, and a variety of other accessible networks.

Intranet

A Local Area Network within an organization, which is designed to look like, and work in the same way as, the Internet. Intranets are essentially private networks, and are not accessible to the public.

Intrusion

The IT equivalent of trespassing. An uninvited and unwelcome entry into a system by an unauthorized source. While Incursions are always seen as Hostile, Intrusions may well be innocent, having occurred in error.

IT Manager

The individual responsible for the technical development, implementation, and/or operational support of a computer system.

ITPM - IT Policy Manual.

The publication that contains IT Policy for the City.

Laptop

A portable computer

Load / System Load

The 'load' on a system refers to the demands placed upon it. The overall load combines many factors and includes:

- Total storage capacity for programs and data
- Number of applications being run concurrently
- Number of concurrent users, peaks, troughs and average
- Number of peripherals: e.g. using a file server as a print server increases demand, as each printed document is 'spooled' to the server's disk before being queued to the printer.

Local Area Network (LAN)

A private communications network owned and operated by the City within one location. This may comprise one or more adjacent buildings, but a local network will normally be connected by fixed cables or short range radio equipment.

Malicious Software (Malware)

Software that causes unauthorized destruction, damage, or unauthorized changes to software, data, or unauthorized use of computer equipment and communication networks.

Media

The physical material which stores computer information. Comes in two basic types - Fixed and Removable and include:

Hard Disk, External Hard Disk, USB Drive, Memory Card, CD, DVD, Floppy Disk, Zip Disk, Magnetic Tape Cartridge, etc.

Need to know

A control principle that ensures that an entity (user, computer processes etc.) is only given sufficient access or authority to complete the entities job function or task.

Non Disclosure Agreement (NDA)

A Non Disclosure Agreement (NDA) is a legally binding document which protects the confidentiality of ideas, designs, plans, concepts or other commercial material. Most often, NDA's are signed by vendors, contractors, consultants and other non-employees who may come into contact with such material.

Official Record

A record with long-term business, legal, or regulatory value.

Operating System

- Software that controls the execution of application programs, resource allocation, scheduling, input/output, and data management
- Computer programs that are primarily or entirely concerned with controlling the computer and its associated hardware, rather than with processing work for users. Computers can operate without application software, but cannot run without an operating system.

Patch

A patch is a software release created to overcome software problems, including glitches and security flaws.

PC

A PC is defined for the purpose of this policy, as a City-assigned personal computer, or workstation.

Phishing

Phishing scams are typically fraudulent email messages appearing to come from legitimate enterprises (e.g., your bank, Internet service provider, the government). These messages usually direct you to a fraudulent web site or otherwise try to get you to divulge private information (e.g., usernames, passwords, account numbers, credit card details, social security numbers, or other account updates). The perpetrators then use this private information to commit identity theft or other crimes.

Policy

Policies are high-level management statements, instructions or business rules that provide guidance to enable individuals to make present and future decisions. Policies are mandatory. Special ITSU management-approval is required when anyone wishes to take a course of action that is not in compliance with policy.

Priority Applications

The sequence of recovery for applications based on their impact to City operations

Private Key

A key used to digitally sign outgoing electronic communication messages/data and decrypt incoming messages/data.

Procedures

Procedures are specific operational steps or manual methods that support a policy or a standard.

For example, a policy could describe the need for back-ups. A standard could define the software to be used to perform back-ups and how to configure this software. A procedure could describe how to use the back-up software, the timing for making back-ups, etc.

Production / Live

When a system is 'in production' or 'live', the system is being used to process active work or transactions, and it is no longer in test/development mode. There must be clear differentiation between systems which are being evaluated, tested, or developed from those which are 'live'.

Project

A plan, including scope, deliverables, work, duration and budget which follows an appropriate Systems Development Methodology.

Publicly Display

To exhibit, hold up, post, or make visible or set out for open view, including, but not limited to, open view on a computer device, computer network, website, or other electronic medium or device, to members of the public or in a public manner.

Public-domain software

Software available to anyone free of charge. Public-domain software is not protected by copyrights. A license or other obligation is not necessary for its legal use. Generally, support is not available. The software can only be obtained in an "as is" condition.

Remote Site

A secure building located outside the range of environmental hazards that could affect the primary computer center.

Remote Storage

A secured storage location in another building with sufficient distance from the original location to ensure its availability in the event that a disaster occurs in the original location.

Risk Management

The process of assessing the threat, the vulnerabilities, and the value of an asset and applying cost effective controls. The purpose of risk management is to balance the risk of loss, damage, or disclosure of an asset against the costs of controls and to select the mix that provides adequate protection without excessive cost in dollars or in the efficient flow of information to those who require ready access to it. The use of a risk management process provides a rational, cost-effective framework as the underlying basis for security decision making.

Separation of duties

A control principle that reduces or eliminates the risk of accidental or intentional misuse of assets (includes business transactions, information etc.) by ensuring that no single individual or process has total control over an asset.

Server

Typically a powerful, special purpose computer which supplies (serves) a network of less powerful machines such as desktop PCs, with applications, data, messaging, communications, information, etc..

Service Level Agreement (SLA)

A Service Level Agreement (SLA) is a contract between two entities (e.g. the City and a vendor or between service units within the City - Data center and Application Owner) to provide a range of support services, up to an agreed minimum standard.

Shareware

A special category of commercial software that is distributed initially without a license. If, after an evaluation period, the user has found the software to be useful, the user may be expected to pay a fee. City users of shareware must pay fees required by a shareware developer. A purchase notification (purchase order or release against a blanket order including The City terms and conditions for software) must be issued to the developer in exchange for a license to continue to use the product. Use of the software must be approved by ITSU management prior to installation or use on City computer systems.

Sign off

An agreement, as evidenced by the customer's signature, that the system or project, meets the specified requirements.

SME

Subject Matter Expert. A person with knowledge in a specific subject area, who is consulted as an expert in that subject.

Standards

Standards are mandatory. They are the next level below policies and include details such as; implementation steps, systems design concepts, software interface specifications, technologies used, and other specifics. Standards may change considerably more often than policies because the associated manual procedures, organizational structures, business processes, and technologies change so rapidly.

Technology Resources

Technologies and information resources used for City information processing, transfer, storage, and communications. Included in this definition are computing and electronic communications devices and services such as workstation computers, laptops, mobile devices (smart phones, tablets, PDAs), networks, printers, electronic communication systems (e-mail, instant messaging, etc.), telephones, digital media, and Internet services. This definition is not all inclusive but rather reflects examples of City of Ann Arbor equipment, supplies, and services.

Tool

A program used for software development or system maintenance. Any program or utility that helps IT personnel or users develop applications or maintain their systems are tools.

Trojan Horse

A software program or command procedure containing malicious hidden code that, when invoked, performs some unwanted function, such as opening a “back door” to the system through which an attacker can connect.

Two-factor Authentication

There are generally three forms of authentication: something a person knows (such as a password), something a person has (such as a bank card or token device), and something a person is (such as a fingerprint or other measure taken from the human body). Two-factor authentication is a type of strong authentication that requires two of the three forms.

User ID (User Name, ID)

A unique identifier that is associated directly with an individual and remains with the person throughout their employment with the City. When the person transfers to a new job, the authorities assigned to the User ID must be changed to reflect access requirements of the new job. Personal User IDs are to be used when accountability for access or changes to data is required.

Users

People who are authorized to use City of Ann Arbor Computer Systems. It includes City employees, volunteers, authorized contractors, and non-regular workforce on assignment to the City.

Virus

A malicious self-replicating program that repeatedly attaches itself to application programs or to any other executable system component to gain control during some phase of execution and to continue the replication process.

Visitor

Individual who is not a regular user of the system and has no registered/recognized User ID or password.

Web Site

A Web site is a collection of Web pages that are generally accessible over the Internet or Intranet using the HTTP protocol. The pages of a website are accessed from a common root URL (the home page) and may reside on the same physical server or multiple servers.

- **Static Web Site**

A web site containing web pages that supply the web browser with information that is pre-formatted and written into the HTML code. Data on a static web page cannot change without changing the source code of the page itself.

- **Dynamic Web Site**

A web site containing web pages that retrieve content from sources outside the HTML code (typically a database), either via choices from the user or page defaults.

Wide Area Network

A communications network that extends beyond the City's immediate premises.

Wi-Fi Protected Access (WPA/WPA2):

A security protocol that encrypts data over the WLAN.

Wired Equivalent Privacy (WEP):

A security protocol that encrypts data over the WLAN. Insecure and deprecated. Wi-Fi Protected Access (WPA/WPA2) should now be used.

Wireless Infrastructure

All components (access points, wireless bridges, wireless repeaters, authentication servers, etc) that create a wireless network whether standalone wireless or providing connectivity to the wired infrastructure.

Worm

A malicious program that uses network connections to spread from system to system automatically. Like a virus, a worm has the ability to infect other systems as well as other programs. A worm will typically expand continuously until it utilizes all available system resources.