INFORMATION TECHNOLOGY POLICY
704 – INFORMATION SECURITY Policy

Policy Title:	**INFORMATION SECURITY POLICY**	Policy Number: APR 704
Effective:	November 1, 2012	
Supersedes:	APR #414 dated 11/97	
Approval:		Page 1 of 5

1. Scope

☒ Full-time
☒ Part-time
☒ Temporary/Contract
☒ Salaried
☒ Union
☒ Independent Contractors
☒ Visitors and Vendors
☒ 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The provisions of this Policy are subject to, and may be superseded by (in the event of a conflict), relevant provisions of applicable collective bargaining agreements between the City and the various collective bargaining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.