INFORMATION TECHNOLOGY AND EQUIPMENT USE POLICY

Overview:

The City of Middletown recognizes the need for technology and the vital role it plays in assisting City employees in delivering services to the public. The City of Middletown has established this policy to ensure that City provided technologies are used appropriately, securely, and for the betterment of the community.

Adopted: 5/13/2019 – Last Revision: 05/7/2019

Definitions:

Information Technology (IT) Staff - The authorized administrators and maintainers of the City's systems. This includes:
- Designated Police Department employees supporting Police Department systems.
- Designated Water and Sewer Department employees supporting SCADA, Industrial Controls, and similar systems.
- Information Technology Department employees supporting Board of Education systems.
- Technology Services Department employees supporting all other systems.
- Sub-contractors, vendors, and other 3rd parties working under the supervision of the above.

System - Any and all technologies, including hardware, software, networks, and services.

Server - A category of device maintained by IT Staff that provides services to multiple users.

Computer - A category of end-user devices which includes laptops, workstations, and thin clients.

Privately Owned Device - Any device that is not issued by the City.

User - Any individual who accesses or operates a system.

End-User - A user who is not a member of the IT Staff.

Hack / Crack - Unauthorized attempt to access or alter a system.

Mobile Device - A category of end-user devices which includes smart phones and tablets.

Network - A system that transmits data between devices.

Guest Network - A network which is made available to the public and restricts devices to communication with the internet and a limited number of internally managed systems.

Public Kiosk - A computer or mobile device which has been made available for members of the public to have limited access to City systems.

Adopted: 5/13/2019 – Last Revision: 05/7/2019

City of Middletown

Technology Services Department
245 deKoven Drive Middletown, CT 06457
TEL: (860) 638-4990 FAX: (860) 638-1928 TDD: (860) 638-4812

Policy

1. City Ownership of Systems and Data
    a. City provided systems and accounts are the property of the City. All messages, documents, and records created, sent, received, or stored on or through City systems are and remain the property of the City and are not the private property of any employee or official. The confidentiality of any message, document, or record should not be assumed.

    b. Any usage of City systems may be monitored as described by the City's Electronic Monitoring Policy.

    c. The City reserves the right to limit or deny access to any City system to prevent damage or loss.

Adopted: 5/13/2019 – Last Revision: 05/7/2019

2. Approved and Prohibited Use of City Systems

a. City systems are provided for City business use. Personal use of City systems during work hours is permitted on a per employee basis by authorization from an employee's supervisor. Personal use of City systems must adhere to this and other City policies. The City reserves the right to restrict personal use on any or all equipment.

b. Violation of any federal or state law (including all copyright laws) is prohibited.

c. Users are prohibited from authoring or transmitting material through City systems regarding any individual which is inflammatory or defamatory.

d. The following uses of City systems are prohibited:
   i. Political campaigning
   ii. Commercial activity (i.e., conducting a private business)
   iii. Collective bargaining purposes, other than by Union officials, the Human Resources Department, the Office of General Counsel, or Mayor's Office

e. The following uses of City systems are prohibited unless approved by the Mayor's Office:
   i. Fundraising activities
   ii. Solicitation for commercial activity, religious or political causes, or the interests of outside organizations
   iii. Broadcast of City-wide non-business related e-mails

f. Users are prohibited from using City systems to transmit messages that violate the City's policies prohibiting sexual harassment or workplace violence. Receipt of any messages violating these policies must be immediately reported by the recipient to his/her department head who in turn will report this to the Director of Human Resources and the Director of Equal Opportunity and Diversity Management.

g. Users are prohibited from using City systems to access offensive websites or other external resources which host offensive content. Specifically, any website or resource which displays pornography, nudity, or any discriminatory content based on race, gender, religion, national origin or any other protected classification of persons shall not be accessed.   The City employs software designed to limit access to such sites and can track each such connection. Any user who visits such a site or resource by accident must inform their department head and IT Staff. If accessing such a site is required for City business (for example, in preparation of legal action), a user requiring such access should inform their department head and the IT Staff.

Adopted: 5/13/2019 – Last Revision: 05/7/2019

City of Middletown

Technology Services Department
245 deKoven Drive Middletown, CT 06457
TEL: (860) 638-4990 FAX: (860) 638-1928 TDD: (860) 638-4812

h. Misrepresenting oneself in any communication or attempting to send any message anonymously through City systems is prohibited.

i. Vandalizing, hacking, or cracking any City system is prohibited. Using City systems to vandalize, hack, or crack any 3rd non-City systems is also prohibited. IT Staff are solely responsible for testing City systems' security and assessing vulnerabilities.

j. Intentionally introducing/downloading malware into any City system is prohibited.

k. Storage of non-work related, personal files (documents, music, pictures, video, etc.) on City servers is prohibited.

3. Record Retention

a. Retention of public records stored on City systems in accordance with Connecticut's records retention laws is the responsibility of the record owners and their department. These records may include, but are not limited to, e-mail messages, documents, and scanned images. Information regarding Connecticut's Municipal Records Management program is available through the CT State Library's website at https://ctstatelibrary.org/publicrecords/municipal.

b. IT Staff maintain backups of City systems for disaster recovery; such backup systems do not relieve users of their responsibility under the law to maintain records.

4. Securing and Maintaining City Systems, Accounts, and Passwords

a. City computers, servers, and mobile devices will have anti-virus, system management tools, and/or other security software and features configured. City networks will have firewalls, email and web filtering, and other security features configured. Attempting to remove, disable, alter, or circumvent such software and security features is prohibited. This includes, but is not limited to, the use of unauthorized web-proxies and 3rd party virtual private networks (VPN).

b. Users of City systems are restricted to those systems to which they have been granted access. Attempting to access a City system to which a user has not been previously granted authorization is prohibited.

c. Installation of software or hardware on City systems without prior approval from IT Staff is prohibited, with the exception of mobile devices. IT Staff are responsible for the installation of software or hardware on City systems; at their discretion, an end-user may be permitted to perform such installation on a case-by-case basis. End-users may install

City of Middletown

Technology Services Department
245 deKoven Drive Middletown, CT 06457
TEL: (860) 638-4990 FAX: (860) 638-1928 TDD: (860) 638-4812

applications on City provided mobile devices provided their usage is in accordance with this and other City policies.

d. Moving or removing equipment comprising City systems without prior approval from IT Staff is prohibited. IT Staff are responsible for moving or removing equipment comprising City systems; at their discretion, an end-user may be permitted to move or remove equipment on a case-by-case basis.

e. Users are prohibited from revealing their user accounts' passwords with anyone or allowing another individual to access City systems with their account/password with the following exceptions:
   i. When under direct orders from his/her department head or direct supervisor. Such a direct order is justifiable only to comply with a legal mandate or to prevent immediate disruption to City business. IT Staff must be informed by the department head or direct supervisor as soon as possible, and the password must be reset once the legal mandate has been fulfilled or the disruption to City business has been resolved.
   ii. When working with IT Staff to diagnose and resolve a problem specifically with a given account on a City system. The password must be reset once the problem has been resolved.

f. All City issued computers and mobile devices must be logged out of or locked by secure method (password, PIN, passcode, biometrics, etc.) when left unattended by the current user. IT Staff may use management software to enforce idle time-outs in compliance with this policy. Public kiosks, in-vehicle terminals in public safety vehicles, and other devices approved by IT Staff are exempt from this requirement.

g. All employees who have been issued accounts for City systems must complete any required cybersecurity training when it is assigned.

5. Procurement of Technology
   a. All new procurement requests for technology needs must be forwarded to IT Staff for review and approval, regardless of funding source. Such review and approval ensures appropriate standardization of products and technology to facilitate support, assessment and mitigation of security risk, and avoidance of redundancy. This includes procurement of:
   - Hardware (desktop, printer, laptop, digital projector, wireless keyboard, etc.)
   - Software
   - Hosted/Cloud services (cloud storage, data warehouses, cloud computing, website hosting, etc.)

Adopted: 5/13/2019 – Last Revision: 05/7/2019

City of Middletown

Technology Services Department
245 deKoven Drive Middletown, CT 06457
TEL: (860) 638-4990 FAX: (860) 638-1928 TDD: (860) 638-4812

- Professional services (consulting, application development, etc.)

   b. Renewals of existing software and services do not require review and approval from IT Staff.

6. Privately Owned Devices

   a. Users may connect privately owned devices to the City's guest networks without prior approval.

   b. Users may connect privately owned devices to the City's e-mail system in accordance with the TECHNOLOGY SERVICES POLICY ON PERSONAL DEVICES CONNECTING TO THE CITY OF MIDDLETOWN'S EXCHANGE SERVICES.

   c. End-users are prohibited from connecting privately owned devices to any other City system without prior authorization from IT Staff.

7. Removal of City-issued Devices from City facilities

   a. City-issued mobile devices may be removed from City facilities by the assigned user.

   b. City-issued computers and other equipment may only be removed from City facilities when the assigned user:
- Requires the equipment to perform City related work from home or while engaged in travel.
- Has received approval from his/her department head.
- Has received approval from IT Staff.

   c. Users are expected to protect such equipment from harmful environments and theft. Should such equipment become damaged, stolen, or otherwise compromised, the user must report the incident to his/her department head and IT Staff as soon as possible. The department head and IT Staff should inform the Office of Risk Management upon receiving the report.

8. Policy Violations

   a. IT Staff may restrict or suspend access for any user who violates this policy.

   b. If IT Staff discover an employee has violated this policy, they will inform that employee's immediate supervisor.

   c. An employee who violates this policy may be subject to disciplinary action up to and including termination of one's employment.

Adopted: 5/13/2019 – Last Revision: 05/7/2019

City of Middletown

Technology Services Department
245 deKoven Drive Middletown, CT 06457
TEL: (860) 638-4990 FAX: (860) 638-1928 TDD: (860) 638-4812

Exclusions: The City's emergency radio and 911 phone system are not considered systems governed by this policy.

City of Middletown

Technology Services Department
245 deKoven Drive Middletown, CT 06457
TEL: (860) 638-4990 FAX: (860) 638-1928 TDD: (860) 638-4812

Policy Acceptance

All users of City systems will be required to sign the Policy Acceptance page indicating they have received and reviewed a copy of this policy prior to being granted access. Employees and elected officials should return the form to Human Resources. Other users should return the form to the IT Staff responsible for granting the appropriate access. This policy is subject to change at any time, with notice to users. A current copy of this policy can be obtained from the Human Resources or Technology Services department.

I, the undersigned, have received and reviewed a copy of Information Technology and Equipment Use Policy.

_____

Signature

_____

Printed Name

_____

Employee Number

_____

Date

Adopted: 5/13/2019 – Last Revision: 05/7/2019