Internet and Computer Usage Policy

Policy No. D-03[1]

The Scope of this policy includes the following individuals:[2]

- ✓ Employees (including Appointed Officials, Probationary Employees, Full-Time At-Will Employees, Part-Time Employees, Temporary Employees, Civil Service Employees, Teamsters Employees, HPOA, HPSA, and IAFF Employees)
- ✓ Full-Time Elected Officials
- ✓ Volunteers

I. PURPOSE

To establish the proper use of the City's information systems and Internet access to ensure that all employees, volunteers, and authorized individuals are responsible, productive users, and are protecting the City's information systems and public image.

II. POLICY APPLICATION

A. Acceptable Use

Employees ("Users") are granted access to City information systems and the Internet to assist them in the performance of their duties. Acceptable use includes activities that enable, support, or benefit the City's mission, its citizens, or employees, and facilitate business processes, communications, and research on behalf of the City. The Internet is provided for legitimate business use in the course of assigned duties and not for any use that is in violation of the "Prohibited Use" section of this policy.

Limited personal Internet use is permitted by this policy during authorized breaks and at the discretion of the employee's supervisor. Personal Internet use is a privilege and

[1] This policy is not to be construed as a contract or an implied contract concerning any employment-related decision or term or condition of employment. The City reserves the right to revise, delete or add to any and all policies, procedures, work rules or benefits stated in this policy at its sole discretion. See Introduction, Administrative Policy No. A-01.

[2] The relevant definitions for the individuals identified in the Scope of this policy are defined in Introduction, Administrative Policy No. A-01.

should not impede the course of City business. Employees should be mindful that they have no expectation of privacy even when using the City's Internet for limited personal use in accordance with this policy.

B. Data Ownership and Monitoring

The City is the owner of all technologies, systems and data stored, transmitted or processed on its network.

The City reserves the right to monitor the use of its computer system or any City-owned device for compliance with these policies and procedures at any time and without prior notice or cause. Such monitoring may include the examination of Internet usage history, e-mail monitoring, and any other information stored or made accessible on the City's computer system. All networks, information assessed, and/or stored on the City's computer system or City-owned devices are subject to monitoring.

This procedure assures compliance with the City's internal policies, addresses legal issues relating to public records, provides internal investigations support, and assists with the management of the City's information system. Employees have no expectation of privacy with regard to their City-owned computer usage. The City reserves the right to determine appropriate usage.

C. Prohibited Use

Unless explicitly authorized as part of a user's job responsibilities, Users shall not:

- access, review, issue, approve, add, delete, or change confidential[3] City data, criminal justice information (CJI), or other regulated data;
- copy, move, transmit, or store confidential City data, personally identifiable information (PII), medical history information or criminal justice information (CJI) onto non-City-owned hard drives or removable electronic media;
- remove non-mobile City-owned devices from City premises without written permission of department director or designee;
- share non-public information about the City, its citizens or employees online, including online social media sites (*e.g.*, Facebook, LinkedIn, Pinterest, etc.); or
- use personal social media accounts to conduct City business.

[3] Confidential data may include, <u>but is not limited to</u>, documents/information containing personal information; records of recreational facility/activity registration where the name, address, telephone number of the applicant are collected; employee medical records; employee personnel records; attorney/client privileged information; and information that is subject to the deliberative process privilege. If an employee is unsure as to whether a document/information is confidential, it is the employee's responsibility to inquire with their supervisor and/or department director to confirm the nature of the document/information.

1. Misuse of City Resource

Employees are not permitted to use the City's computer systems or Internet connection for personal gain, to benefit another, to market or solicit personal business ventures, to advocate any religious, political, ideological, philosophical, special-interest, or other such personal causes.

Employees are prohibited from accessing, downloading, reviewing, or exchanging any content that may reasonably be considered offensive to any employee. Offensive material includes, but is not limited to, pornography, sexual comments, jokes or images, racial slurs, gender-specific comments, or any comments, jokes or images that would offend someone on the basis race, color, hair texture and protective hairstyles, religion, sex, pregnancy, age, national origin or ancestry, disability, veteran status, sexual orientation, gender identity or expression, status as HIV positive, genetic information, or any other consideration protected by federal, state, or local laws. Any use of the Internet to harass or discriminate is unlawful and strictly prohibited by the City.

2. Software

Employees may not download or install software from the Internet without approval from the Department of Information Technology (DoIT). Employees are prohibited from accessing, downloading, exchanging, or using pirated software, games, stolen passwords, hacking software, or any other inappropriate software material on the City's computer system. Installation of software on City-owned devices may only be performed by the DoIT or its designees, or as authorized by the DoIT. Installation of City-owned software onto employee-owned devices is prohibited unless first approved the DoIT.

Employees may not bypass technical or security controls or configure software or hardware to intentionally allow access to unauthorized Users.

3. Non-City Owned Devices

Connecting non-City owned devices, or systems physically or via any wireless means to the City internal network or data resources is prohibited. Employees are permitted to remotely connect a personally owned device via the DoIT approved remote methods to the City's internal network or data resources provided those devices meet the DoIT security standards.

4. City Email

Employees may not use their City username, City email addresses, or City passwords to sign up for third-party website accounts or services, including

health and banking accounts, social media or any others, unless authorized by the DoIT. Employees may not subscribe to any non-work related list servers or mailing lists using their City-owned email address.

5. Mobile Devices

Employees are not permitted to use jailbroken or rooted mobile devices to access any City technology resources. User shall not download, install, or use non-work-related applications on City-owned mobile devices.

6. Confidential Data

Employees may not distribute confidential City data, criminal justice information (CJI), personally identifiable information (PII), cardholder data (PCI data), health or employee data or other restricted information to unauthorized persons or parties.

7. Data Storage

Employees may not copy or store credit or debit card data (PCI data) electronically. Lost or stolen credit card information as part of a Public Safety case is exempt from this requirement. Employees may not place City software, internal memoranda, or other information on any publicly accessible Internet computer unless the posting of this material has first been approved by the City Manager or designee and the City Attorney or designee. All non-public record information must be encrypted in a manner approved by the DoIT before it is transmitted via the Internet.

8. Adherence

Failure to comply with the policies and procedures outlined herein may lead to revocation of system access privileges and disciplinary action, up to and including termination, in accordance with the provisions of any applicable collective bargaining agreement and the Civil Service Rules. The City does not consider conduct in violation of this policy to be within the course and scope of employment. Accordingly, to the extent permitted by law, the City reserves the right not to provide a defense or pay damages assessed against employees for conduct in violation of this policy.

The City reserves the right to terminate, without notice to the user, any active connections or accounts that are deemed to pose a security risk or are in violation of this or any associated policy.

D. CYBERSECURITY TRAINING AND TESTING

1. Training Program Determination and Cadence

The City requires annual cybersecurity training for all employees with access to the City's network. Additional annual role-based security awareness training is required for users whose responsibilities require access to information subject to HIPAA, PCI-DSS, CJIS, NRS and other relevant regulatory or contractual compliance programs.

2. Phishing Tests

The City will conduct regular, unannounced phishing tests for all employees with access to the City's network. Regular reports will be provided to department heads regarding test success and failure rates, highlighting users of concern. Each user who fails phishing tests 50% or more each month is assigned remedial cybersecurity training.

3. Training Cadence and Compliance

Supervisors will be notified of their direct report's training completion status, both annual and remedial. In addition department directors will also be notified when training is past due. The department heads and supervisors will continue to receive notifications until completion or remedial action is taken. Failure to complete training by the deadline, or continuing to fail phishing tests despite additional training, will be subject to progressive discipline, up to and including revocation of internet and email privileges, disabling of the account, or termination of the employee.

III. APPROVAL

APPROVED BY:
Richard Derrick, City Manager/CEO

REVIEWED BY:
Nicholas Vaskov, City Attorney
Brooke Stream, Director of Human Resources

Record of approved document can be obtained through the Human Resources Department.

ORIGINAL EFFECTIVE DATE: 2/16/2016
REVISION DATE(S): 12/20/2023