ELECTRONICS USE POLICY

Updated October 28, 2019

CITY OF JAMESTOWN
ELECTRONIC SYSTEMS USE POLICY
EFFECTIVE: **July 11, 2018**

Acceptable Use

1. PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at the City of Jamestown. These rules are in place to protect the employee and City of Jamestown. Inappropriate use exposes the City of Jamestown to risks including virus attacks, compromise of network systems and services, and legal issues.

2. SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources to conduct City of Jamestown business or interact with internal networks and business systems, whether owned or leased by The City of Jamestown, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at the City of Jamestown and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the City of Jamestown policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at the City of Jamestown, including all personnel affiliated with third parties. This policy applies to all electronic equipment that is owned or leased by the City of Jamestown.

Electronic systems shall be defined as all hardware, software and tools owned or operated in whole or in part by the City of Jamestown. This includes shared information systems and those available equipment for official use by City of Jamestown employees. Electronic systems shall include, but not be limited to, personal computers, networking computers, mobile data, photo imaging, electronic mail, voice mail, calendaring, the Internet, cell phones and pagers.

3. POLICY

3.1 General Use and Ownership

1. The City of Jamestown proprietary information stored on electronic and computing devices whether owned or leased by the City of Jamestown, the employee or a third party, remains the sole property of the City of Jamestown.

2. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of City of Jamestown proprietary information.

3. You may access, use or share City of Jamestown proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

5. For security and network maintenance purposes, authorized individuals within City of Jamestown may monitor equipment, systems and network traffic at any time.

6. The City of Jamestown reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.2 Security and Proprietary Information

1. All mobile and computing devices that connect to the internal network must be approved by the Director of Information Technology.

2. System level and user level passwords must be kept confidential. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

3. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 60 minutes or less. You must lock the screen or log off when the device is unattended.

4. Postings by employees from the City of Jamestown email address to newsgroups is strictly prohibited unless posting is in the course of business duties.

3.3 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City of Jamestown.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which City of Jamestown or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting City of Jamestown business, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology. The appropriate management should be consulted prior to export of any material that is in question.

5. Using unauthorized media for transferring files. All media that is not purchased through the City of Jamestown must be approved by the IT Director.

6. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

7. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

8. Using a City of Jamestown computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

9. Making fraudulent offers of products, items, or services originating from any City of Jamestown account.

10. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

11. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this

section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

12. Port scanning or security scanning is expressly prohibited unless approved by the Director of Information Technology and Communications.

13. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

14. Circumventing user authentication or security of any host, network or account.

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, City of Jamestown employees to parties outside the City of Jamestown.

3.4 Email and Communication Activities

The purpose of this section is to ensure the proper use of the City of Jamestown's email system and make users aware of what the City of Jamestown deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within the City of Jamestown Network. When using company resources to access and use email, users must realize they represent the City of Jamestown. Questions may be addressed to the IT Department

3.4.1 Authorized Use

1. All use of email must be consistent with City of Jamestown policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

2. The City of Jamestown email account should be used primarily for City of Jamestown business-related purposes; personal communication is permitted on a limited basis, but non-City of Jamestown related commercial uses are prohibited.

3. The City of Jamestown may monitor messages without prior notice. The City of Jamestown is not obliged to monitor email messages.

4. City of Jamestown employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.

5. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

3.4.2 Unauthorized Use

1. The City of Jamestown email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any City of Jamestown employee should report the matter to their supervisor immediately.

2. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct City of Jamestown business, to create or memorialize any binding transactions, or to store or retain email on behalf of the City of Jamestown. Such communications and transactions should be conducted through proper channels using City of Jamestown-approved documentation.

3. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

4. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

5. Unauthorized use, or forging, of email header information.

6. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

7. Creating or forwarding "chain letters" or "pyramid" schemes of any type.

8. Use of unsolicited email originating from within City of Jamestown's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the City of Jamestown or connected via City of Jamestown's network.

9. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

10. Unless determined to be otherwise impractical by the Director of Information Technology or the Corporation Counsel, City business transacted via email must be

conducted through an employee's official city email address. It is inappropriate and violation of State Law to transact official public business through private email accounts.

3.5 Blogging and Social Media

1. Blogging by employees, whether using City of Jamestown's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of City of Jamestown's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate City of Jamestown's policy, is not detrimental to City of Jamestown's best interests, and does not interfere with an employee's regular work duties. Blogging from City of Jamestown's systems is also subject to monitoring.

2. The City of Jamestown's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any City of Jamestown confidential or proprietary information, trade secrets or any other material covered by City of Jamestown's Confidential Information policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the City of Jamestown and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by City of Jamestown's *Non-Discrimination and Anti-Harassment* policy.

4. Employees may also not attribute personal statements, opinions or beliefs to the City of Jamestown when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the City of Jamestown. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, City of Jamestown's trademarks, logos and any other City of Jamestown intellectual property may also not be used in connection with any blogging activity

3.6 Remote Access

Remote access to our corporate network can be arranged with approval from the Director of IT and your department head.

1. Authorized Users are responsible for preventing access to any City of Jamestown computer resources or data by non-Authorized Users. Performance of illegal activities through the City of Jamestown network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access.

2. Remote access is secured with encryption and a Virtual Private Network

3. Authorized Users shall protect their login and password, even from family members.

4. While using a City of Jamestown-owned computer to remotely connect to City of Jamestown's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

5. All hosts that are connected to City of Jamestown's internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.

6. Personal equipment used to connect to City of Jamestown's networks must meet the requirements of City of Jamestown-owned equipment for remote access.

3.7 Software Installation

The purpose of this section is to outline the requirements around installation software on City of Jamestown computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within City of Jamestown's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

1. Employees may not install software on the City of Jamestown's computing devices operated within the City of Jamestown's network.

2. Software requests must be approved by the Department Head and then be made to the Information Technology department in writing or via email.

3. The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

4. An employee found to have violated this policy may be subject to disciplinary action.

3.9 Internet Use

The purpose of this section is to define the appropriate uses of the Internet by City of Jamestown employees and affiliates. All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The City of Jamestown is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

3.9.1 Acceptable Access

1. Internet access will only be granted if the employee signs this policy and completes the Cybersecurity training.

2. The Internet should only be sued for business purposes.

3. To perform communications with outside organizations

3.9.2 Unacceptable Access

1. Streaming audio and video for non-official city business is strictly prohibited.

2. The Internet shall not be used for any illegal, improper, unprofessional or illicit purposes. The transmission of any material in violation of City, State, or Federal law or regulation is prohibited. This includes, but is not limited to, copyrighted, obscene, pornographic, gambling, threatening or intimidating materials, etc.

3. Intentional misuse shall subject the user to termination of access rights and disciplinary action.

All City of Jamestown employees who access electronic systems are required to complete Cybersecurity training and sign this form. If you choose not to complete the training or sign this form you will not be eligible to use the City's electronic systems.

Electronic Systems Use Policy
Acceptance Statement

EFFECTIVE: **July 11, 2018**

I, the undersigned, have read and understand the rules and regulations as outlined in the Electronic Systems Use Policy for the City of Jamestown. I agree to abide by the terms and conditions laid out in the document.

_____

City of Jamestown Employee Print Name

_____ _____

City of Jamestown Employee Signature **Date**

_____ _____

Witness (Department Head or Supervisor) **Date**

ALL FORMS MUST BE RETURNED IMMEDIATELY TO THE INFORMATION TECHNOLOGY DEPARTMENT MARK DEAN BEFORE YOU CAN USE THE COMPUTER SYSTEM.