Technology Acceptable Use Policy

INTRODUCTION

The City of Baltimore ("City") is committed to responsible stewardship of the City's information technology ("IT") resources. To achieve this objective, the City created this Technology Acceptable Use Policy ("Policy") to ensure compliance with best practices in managing IT resources. This Policy will improve the City's ability to serve the community, strengthen resident data protection, and mitigate the impact of future cyberattacks. Use of City's IT resources may provide user access to valuable organizational resources, to sensitive and critical data, and to internal and external networks. Use of the City's computer and network resources is a privilege. The City expects users of the City's IT resources to act in a responsible, professional, ethical, and law-abiding manner.

I. PURPOSE

This Policy establishes safeguards and controls to prevent the loss, abuse, and theft of information, data and equipment owned by or leased to the City. Adherence to this Policy promotes the mitigation of financial loss related to IT security incidents and the likelihood of personal or sensitive information loss. The agency head or designee bears responsibility for implementing this Policy.

II. SCOPE

This Policy applies to the City of Baltimore's computing, networking, digital technology, operational technology ("OT"), supervisory control and data acquisition ("SCADA"), telephony, digital assets and digital files or information that may be owned, leased, or managed by the City ("City IT resources").

This Policy applies to all users of the City's IT resources. Specifically, this Policy applies to anyone that obtains access to the City's IT resources including individuals who connect to the City's IT resources by wire or wirelessly using personally owned devices. Individuals covered by this Policy are collectively referred to as "users" and include full and part-time employees, contractors, interns, partners, visitors, and customers.

III. USER RESPONSIBILITIES

Users of the City's IT resources are granted access to certain IT resources that are required to perform work duties, including access to computer systems, servers, software, databases, files, folders, documents, telephony, email, voice mail systems, smart phone applications, and the internet.

Users are responsible for knowing, understanding and following this Policy. Users are responsible for exercising common sense and good judgment in adherence of this Policy. An action deemed technically possible does not mean that it is appropriate or permitted.

Users are responsible for knowing, understanding, and following all data protection and privacy laws, regulations, and industry standards that apply to their job duties. The City and its users are responsible for the safe handling and protection of sensitive data as required by any applicable laws, regulations, or industry best practices. Examples of data protection laws, regulations, and industry best practices include the Health Information and Portability Accountability Act ("HIPAA"), the Criminal Justice Information Services ("CJIS"), and the Payment Card Industry Data Security Standard ("PCI"). In addition, users are responsible for knowing, understanding and following the prohibitions on disclosure found in the Maryland Public Information Act and other federal, state, and local privacy laws. Agencies are responsible for ensuring users are trained on any relevant data protection regulations or best practices that apply to their job duties.

As representatives of the City, users are responsible for all content created utilizing the City's IT resources including emails, texts, chats, audio, voice mail, faxes, images, whether digital or hard copy. Creating fraudulent, harassing, or sexually explicit content is prohibited. Content that may be inappropriate or offensive based on race, sex, religion, national origin, physical attributes, disabilities, sexual preferences, age, or other characteristics protected by law are prohibited. Users are required to report offensive content to their supervisors or Human Resources. Users shall not create or transmit content under an assumed name or attempt to obscure the origin of any content.

IV. ACCEPTABLE USE

- Only use authorized IT resources specific to stated job functions or responsibilities.
- The City will provide users with a unique username that contains identifiable information individual to each user. Specifically, each username contains the first and last name of the user that appears in the Human Capital Management system.
- Users shall adhere to the City's password policy, which requires:

    i. minimum of 12 characters;
    ii. at least 1 lower-case letter;
    iii. at least 1 upper-case letter;
    iv. at least 1number; and
    v. at least 1 special character.

- Users must protect all passwords used to secure the City's IT resources against unauthorized access and use. Never share a password with anyone.
- Users are responsible and accountable for appropriate use of all IT resources assigned to them.
- The City's IT resources shall only be used for City business. Incidental personal use of the system may be permitted if it:

    i. is done on the user's personal time during a lunch break or another manager approved break;
    ii. does not consume more than a trivial amount of City IT resources that could otherwise be used for City business;
    iii. does not interfere with a user's' productivity;
    iv. does not take the place of any City business; and
    v. does not otherwise violate this Policy, or any other applicable law, regulation, or procedure.

- Users shall not use the City's IT resources for personal gain or advancement of a user's own personal views; to operate a business; political campaigning; fund raising; or to solicit non-City business.
- Sending chain letters, mass mailings, jokes, comics, or non-job-related computer graphics is prohibited.
- Users shall not provide resources or other forms of assistance that facilitate any unauthorized access to the City's IT resources.

- The City is bound by contractual and licensing agreements with regard to third-party resources, such as software programs. Users must comply with all such agreements when using third-party resources.
- Users shall not attempt to access or provide resources to access restricted portions of the network, an operating system, security software, or other administrative applications without appropriate authorization by the system owner or administrator.
- Users shall comply with the policies and guidelines for all of the City's IT resources to which they have been granted access. When other policies are more restrictive than this Policy, the more restrictive policy governs.
- Users may not engage in deliberate activity to degrade the performance of the City's IT resources, deprive an authorized user access to the City's IT resources, obtain extra City IT resources beyond those allocated, or circumvent the City's IT resources security measures.
- Users shall not attempt to bypass any security control unless they have been specifically authorized to do so, in writing, by the Chief Information Officer ("CIO") or the Chief Information Security Officer ("CISO").
- Users who are provided with City-issued devices, such as desktops, laptops, phones, hotspots, or any other device, are responsible for taking care of each device and returning each device to the City in good working order when it is time for a device refresh or upon completion of employment or their contract. Good working order includes not wiping the City's data from the device or preventing City IT administrators from accessing the device upon return. AM 241-2-1 provides the City's policy for returning equipment and AM 241-2-2 provides a checklist.

V. OTHER PROVISIONS

- **Software** – A user shall not install applications obtained from outside sources on the City's IT resources. Software or applications that have not been vetted or reviewed by BCIT may contain malicious software (malware). In addition, the City must abide by software vendor license agreements.
- **Games and Streaming Media** – Users are prohibited from downloading games or using the City's IT resources to play or participate in on-line gaming outside of agency sponsored team-building or educational events. In addition, users are prohibited from streaming entertainment media on the City's IT resources. Streaming entertainment uses valuable network bandwidth that could impact the productivity of other users or negatively impact other City's IT resources. City issued phones or WiFi Hotspots shall not be used for on-line gaming, except as stated above, or to stream media for personal use.
- **Copyright** – Users shall comply with all copyright laws and applicable license requirements that may apply to City IT resources, including software, files, graphics, images, messages, and other content.
- **Hardware** – Users may connect their personal device (laptop, phone, tablet, etc.) to the City's guest Wi-Fi. However, users are prohibited from adding or installing hardware to the City's IT resources without following the relevant BCIT process. Examples include installing routers, wireless/Wi-Fi routers, Wi-Fi devices, Bluetooth enabled devices, Alexa, Google, or similar smart assistants, network switches, sensors, or cameras.
- **Blocking Web or Internet Content** – The City reserves the right to block content that is considered offensive, sites that could pose a risk to the City's IT resources or contribute to an environment that is not welcoming.

- **Sensitive and Protected Data –** The City is a steward of all of its data, including sensitive and protected data. Users shall not send or transmit sensitive or protected data without appropriate authorization. Users shall check with their supervisor to understand and follow all requirements for handling sensitive and protected data. Sensitive and protected data authorized for distribution outside of City IT resources shall be transmitted over encrypted communication channels. Contact Infosec infosec@baltimorecity.gov for guidance on how to safely transmit sensitive or protected data.
- **Administrative Privileges or Privileged Access –** The City typically grants special privileges or access to system administrators, network administrators, staff performing computing account administration, or other users whose job duties require special privileges or access to perform security duties, maintain the system, or to diagnose and address system issues. The need for administrative privileges or privileged access must be documented in the user's job description or contract and approved by a manager. Users with administrative privileges or privileged access must take training and sign an acknowledgement of their responsibilities on an annual basis.

VI. OWNERSHIP AND PRIVACY

The City owns all rights to all content created, updated, or maintained on City IT resources unless ownership rights are reserved in writing to a third party or unless federal copyright or other laws provide for different rights. Users have no expectation of privacy when using City IT resources. The City reserves the right to access and monitor all messages, files, logs, and content created using City IT resources. Communications or content may be subject to disclosure to BCIT, the Office of Inspector General ("OIG"), the Law Department, law enforcement, or the Department of Human Resources ("DHR"), to the fullest extent allowed by law.

VII. COMPLIANCE

Users found in violation of this Technology Acceptable Use Policy are subject to disciplinary action up to and including restriction, possible loss of privileges, suspension, or termination. If necessary, the City will notify the City's Law Department, OIG, or law enforcement of any legal violations.

VIII. EMPLOYEE/CONTRACTOR/USER ACKNOWLEDGEMENT

I have read, or have had read to me, this Technology Acceptable Use Policy. I understand it is my responsibility to adhere to the requirements in this document.

____

Employee / Contractor / User's Printed Name

____ ______________________

Employee / Contractor / User's Signature Date