CITY OF PROVIDENCE

# 5.1 INFORMATION AND SYSTEMS SECURITY POLICY

## Purpose

This policy outlines the standards and expectations for the use of the City's information and technology resources. The goal is to provide guidance on safe, secure access to resources needed to conduct City business, while protecting the integrity of the network, data, and devices which manage these services.

## Scope

This policy applies to all users - employees, interns, fellows, volunteers and contractors of the City of Providence who are provided with access to any IT resources. It also applies to granted access to City resources from personal computers or mobile devices.

This policy applies to all City of Providence IT resources, including computers, mobile devices, printers, peripherals (e.g., keyboards, mice, monitors, storage devices), security equipment, Internet of Things (IoT) devices, electronic control systems, software applications, electronic data, local and wide area networks, email systems, and internet usage.

## Policy

Using any City IT resource constitutes acceptance of the terms of this policy and any corresponding policies such as those prohibiting harassment, discrimination, offensive conduct, or inappropriate behavior.

1. **User Responsibilities:**
   A. It is the responsibility of any person using City IT resources to read, understand, and comply with this policy. Users are expected to exercise reasonable judgment in interpreting this policy and making decisions about the use of City IT resources.
      1. Use IT resources only for authorized work-related activities.
      2. Protect the City's data and systems from unauthorized access or disclosure.
      3. Immediately report any suspected security incidents or policy violations.
      4. Adhere to all applicable laws, policies, and regulations.
   B. Any person with questions regarding the application or meaning of this policy should seek clarification from your supervisor, department director or the Department of Information Technology ("IT").

2. **Training:**
   A. The IT department hosts a variety of training resources, including regular Cybersecurity Training, online help, and direct access to IT staff who specialize in a variety of business applications and services. All users are expected to participate in Cybersecurity Training and use these lessons to protect business resources as well as personal electronic assets.
   B. Supervisors are encouraged to reach out to IT for development of training programs to address their department needs.

3. **Unacceptable Uses of City IT Resources**
   A. All resources provided by the IT department (such as computers, networks, software) are valuable assets that need to be used responsibly and efficiently.
   B. Unacceptable use can lead to security breaches, malware infections, system downtime and data leaks, putting the organization and its users at risk. The City must also comply with various laws, regulations, and industry standards regarding data privacy, intellectual property, and cybersecurity. Unacceptable use can damage the City's reputation by causing disruptions, leaks of sensitive information, or engaging in illegal or unethical activities. Unacceptable use can harm other users by causing disruptions, harassment, or the spread of malicious software.

C. Therefore, this list is not exhaustive, however it is unacceptable for any person to use IT resources in the following manner(s):

1. **Illegal or Unauthorized Activities**
    1. Assisting in any illegal act, including violations of criminal or civil laws or regulations (state or federal).
    2. Gaining or attempting to gain unauthorized access to any computer, network, or communications not related to your ordinary or customary duties or responsibilities.
    3. Sharing user accounts or physical access credentials or using those belonging to others to access IT resources or unauthorized areas.
    4. To deliberately access communications that are not addressed to you or intercept communications intended for other people.
2. **Security and Network Integrity**
    1. Causing interference with or disruption of network users or resources, including the transmission of computer viruses or other harmful programs.
    2. Downloading, installing, or using software, programs, or applications on City systems without prior approval from the Information Technology Department.
    3. Sharing confidential information or Controlled Unclassified Information (CUI) without proper authorization.
3. **Inappropriate or Non-Official Use**
    1. Engaging in political (unrelated to official duties), religious, or commercial activities.
    2. Soliciting or attempting to convert individuals or organizations for non-job-related purposes.
    3. Accessing online gambling, social networking, or dating sites (e.g., Facebook, Instagram, Tinder), unless reasonably related to job duties. Refer to the Social Media Policy for more information.
    4. Accessing, installing, or using computer games.
4. **Harassment, Defamation, or Misrepresentation**
    1. Sending threatening or harassing messages, whether sexual or otherwise.
    2. Accessing or sharing sexually explicit, obscene, or otherwise inappropriate materials.
    3. To publish or transmit any content that constitutes libel, slander, or defamation of character.
    4. Misrepresenting the City or an employee's role within it.
    5. Playing pranks that could reasonably affect another employee's performance or workplace conditions.
5. **Intellectual Property Violations**
    Infringing on intellectual property rights. (i.e., trademark, copyright)

4. **Data Confidentiality**

A. In the course of their duties, City employees and contractors may have access to confidential or proprietary information. This includes personal data about identifiable individuals, commercial information about organizations, and Controlled Unclassified Information (CUI).

**B. Examples of CUI include:**

1. Personally Identifiable Information (PII)
2. HIPAA-protected health data
3. Law Enforcement Sensitive (LES) information
4. Financial records
5. Confidential, privileged communications between the City and its attorneys

**C. Access to such information is strictly regulated:**

1. Employees and contractors may only access confidential data, including CUI, if it is necessary for the performance of their job duties.
2. Even if access is authorized, users are prohibited from copying or disseminating confidential information unless it is essential to fulfill their responsibilities.
3. If there is any uncertainty about whether certain information may be shared, employees must consult the City Solicitor's Office before proceeding.

D. While most documents and records generated during normal business operations are considered public records and subject to APRA (Public Records Law), many exceptions exist. All public records requests must be referred to and handled by the Law Department's APRA team to ensure no confidential information is inadvertently released.

5. **Use of Personal Accounts**
   A. Employees are strictly prohibited from using personal or non-City-provided accounts, such as personal email, messaging, or file-sharing services, to conduct City business, transmit data, or communicate official information; provided, however, that it shall not be a violation of this policy for employees to communicate with each other regarding work related matters via text messages through their personal devices. City business and data must never be uploaded to, shared through, or distributed via personal accounts under any circumstances.
   B. To support secure and effective operations, the City provides a wide range of approved applications and resources for conducting official communications and transactions. All employees have access to these tools to ensure business is conducted through secure, authorized channels.
   C. The Information Technology Department welcomes feedback and encourages suggestions for improving existing systems or implementing new tools to better support City operations.

6. **Copyright Protection**
   A. Computer software and digital content are protected forms of intellectual property. Software publishers often take active measures to enforce their rights, and similar legal protections apply to online materials, including website text, images, and graphics.
   B. All users are expected to respect intellectual property rights and to exercise caution and good judgment when copying, sharing, or distributing software or content that may be copyrighted.
   C. If there is any uncertainty about whether an action may violate copyright or intellectual property laws, users should consult the Information Technology Department before proceeding.

7. **Network Integrity and Security**
   A. Users must take reasonable precautions to prevent the introduction of malicious software or unauthorized programs into the City's local or wide area networks. Although virus-scanning tools are in place to inspect software from the internet or other unverified sources, these tools are not infallible.
   B. The following measures should be observed:
      1. Executable files (program files that end in ".exe") should not be stored on or run from network drives.
      2. Emails from unknown senders, particularly with attachments and links, should be deleted without opening.
   C. Most City computers are connected to a shared local area network. To protect this infrastructure, users must adhere to the following security practices:
      1. Do not share login credentials. User IDs and passwords are assigned to individuals and must remain confidential.
      2. Never use credentials assigned to another person to access City systems or equipment.
      3. Immediately notify the IT Department if you believe your password or passphrase has been compromised.
      4. Do not reuse City network credentials for any non-City accounts.
      5. Lock your computer or log off whenever leaving it unattended, regardless of the duration.
      6. Be alert to phishing emails or credential requests. If you receive any suspicious communication asking for login information, report it to the IT Department by email helpdesk@providenceri.gov and then deleting the email.

8. **Non-City Regulated Equipment**
   Personal or non-City regulated equipment must never be connected to the City's physical network infrastructure. This includes, but is not limited to, personal laptops, computers, routers, switches, and Wi-Fi access points.

9. **Multi-Factor Authentication (MFA)**
   Some network or business application accounts may require multi-factor authentication (MFA), such as text messages or authentication apps generating one-time codes. The use of personal mobile phones for MFA is permitted. Any phone number provided for authentication will be treated as confidential and used solely by the IT Department for security purposes.

10. **Network Resource Usage**
    Applications that consume excessive network, server resources, or internet bandwidth—or that degrade overall network performance—may be blocked. If a blocked application or website is required for business purposes, users should contact the IT Department for assistance.

11. **Inactive Equipment**
    City-owned computer equipment with no user activity for 30 days may be disabled by the IT Department.

12. **Communication, Messaging, and Email**
    A. Messaging systems include email, text messaging, online platforms, and any communication tools provided by the City or used for official City business.

    **B. Format/ Restrictions:**
    1. City email addresses (e.g., *yourname@providenceri.gov*) represent the City and must be treated like official City letterhead.
    2. All messages must be professional, courteous, and appropriate for public or official record.
    3. Assume all messages can be stored, forwarded, or printed—do not include content you wouldn't write in an official memorandum.
    4. Users must not send electronic mail to all other employee users through the use of the "All-Staff" address group unless expressly authorized by management to do so.
    5. Messages soliciting funds or support for outside organizations are prohibited - even if such is not for personal gain - except as authorized by the Mayor's office or Department of People and Culture.

    Please refer to the Use of Email Policy covering use of email by employees for additional regulations and guidelines

13. **Monitoring and Privacy**
    A. All City IT resources and data are the property of the City of Providence and must be used in accordance with this policy. The City reserves the right, at its discretion, to inspect any City-owned computer or device, including all data stored on it and any data sent or received—such as internet activity, emails, and other communications.

    B. To ensure proper operation and security, network administrators routinely monitor network traffic. By using City IT resources, users expressly consent to this monitoring and inspection, including review of data created, received, or transmitted and websites accessed.

    C. Whether by email, text, or other platforms related to any matter in which the City holds jurisdiction, control, supervision, or advisory authority may be considered public records under the Rhode Island Access to Public Records Act (APRA). These records may be subject to public disclosure. Employees may be asked to provide copies of work-related text messages in response to public records requests whether it be a City issued device or personal device. However, under no circumstances will an employee be required to turn over their personal phone for inspection or retrieval of public records unless compelled by court order.

14. **City Wi-Fi Use**
    A. City Wi-Fi is provided to support visitors in City buildings and to enable staff access to networks while working outside their regular office locations.

    B. Employees may use City Wi-Fi for personal purposes on personal mobile devices only during designated break times, lunch periods, or outside of regular working hours. However, personal use is strictly prohibited for the following activities:
        1. Operating a personal business
        2. Performing work for another employer
        3. Volunteering or working for a political candidate

    C. Personal use must never interfere with job responsibilities or disrupt workplace operations. Use of City Wi-Fi is also governed by applicable portions of this policy, such as its limitations to accessing inappropriate websites, downloading games or disseminating offensive material.

15. **Remote Access**
    Please refer to the Remote Access Virtual Private Network (VPN) Security Policy covering VPN Access by employees for additional regulations and guidelines.

16. **Mobile Device Management**
    Please refer to the Laptop Computer and Mobile Device Policy covering the use of mobile computers by employees for additional regulations and guidelines

17. **Social Networking and Publication**
    Please refer to the Social Media Policy covering acceptable uses of social media, considerations to take when referencing the City of Providence, individual departments, coworkers or business topics in public forums or social networks.

18. **Compliance**
    A. Failure to adhere to the provisions of this policy will result in corrective or disciplinary action in accordance with City policies and applicable law.
    B. The Department of Information and Technology (IT) and the Department of People and Culture (DPC) shall monitor compliance with this policy and may conduct periodic audits to ensure consistent application and prevent misuse.
    C. Any discrepancies or violations identified through audits or employee complaints will be investigated and addressed promptly.

## Related Information:

The City of Providence reserves the right to monitor, review, audit, and disclose any messages sent, received, or stored on the City's email system, at its sole discretion and for any legitimate purpose. The City may also block or restrict access to public websites or non-City email accounts that violate this policy. Additionally, all use of City IT resources—including access to City-owned hardware, software, and any computer-related activity conducted through City systems or accounts—may be reviewed or audited to ensure compliance with applicable policies and regulations.

## Related Policies:

Laptop Computer and Mobile Device Policy
Remote Access Virtual Private Network (VPN) Security Policy
Email Use Policy
Electronic Signatures
Artificial Intelligence (AI) Policy
Social Media Policy