CITY OF PROVIDENCE

5.5 EMAIL USE POLICY

Purpose

This policy establishes rules for the acceptable use of the City of Providence email system to ensure secure, efficient, and appropriate communication for conducting official City business.

Scope

This policy applies to all City of Providence employees, interns, contractors, fellows, volunteers and any other individuals granted access to a City-issued email account or who communicate on behalf of the City using electronic mail.

Policy

1. **Preamble**

   City employees must use the provided government domain email account assigned to them when using email to conduct City business or City-related business activities. Gov domains are different because they're only available to U.S.-based government organizations. This special type of domain makes it easy to identify governments on the internet and helps the public identify that the email in their inbox is genuine.

2. **Eligibility**

   A. The following are eligible for a City email account:
      1. Active City employees
      2. Contractors and consultants conducting business with services rendered to and on behalf of the City
      3. Volunteers engaged in work on behalf the City
      4. Retirees acting for or on behalf of the City in a capacity which warrants the use of a City email account to conduct City business

   B. There must be a valid necessity to warrant access to a City email account and such access is not permitted for personal reasons as prescribed herein.

3. **Conditions and Obligations**

   Conditions and obligations for use of the City of Providence email services include:

   A. City email is intended primarily for transactional communication and not as a long-term storage solution or system of record. When necessary, emails and attachments must be transferred to appropriate electronic records management systems in accordance with the City's official records retention policies.

   B. Use of a City email account for any personal business or commercial activity is strictly prohibited.

   C. Employees must not use personal passwords—such as those associated with non-City email, banking, shopping, or social media accounts—on City devices or within City-managed systems. Doing so increases the risk of credential compromise and undermines the security of the City's technology environment. Users should change their passwords at certain intervals of time and take precautions to prevent unauthorized access to their mailboxes, such as logging off when their computer is unattended.

   D. Automatic forwarding of City email to a non-city email account is prohibited.

   E. For security purposes, access to City email accounts will require a multifactor authentication (MFA) process. This additional verification step is mandatory to ensure secure login and protect against unauthorized access to City communications.

   F. The email transmission of highly sensitive Controlled Unclassified Information (CUI)—such as but not limited to, Social Security numbers, medical or patient data, financial account numbers, or credit card

information—to external email addresses is strictly prohibited unless done through City-approved encrypted methods.

G. Highly sensitive CUI must not be stored in a City email account. Email messages or attachments containing CUI must be deleted or moved to an appropriate storage location as soon as possible or within 30 days of receipt or transmission.

H. City email accounts will be deactivated and subsequently deleted once the assigned user is no longer authorized to access City email (e.g., upon termination, resignation, or end of contract).

I. Supervisors are responsible for working with departing employees to ensure that any emails are essential to business continuity—especially those involving legal matters, proprietary or confidential information, compliance correspondence, or recordkeeping—are transferred to an appropriate custodian prior to the employee's last day. The City reserves the right to access, review, copy or delete all messages for legitimate business and disciplinary purposes and disclose them to any party it deems appropriate.

4. **Compliance**

A. Failure to comply with the conditions and obligations outlined in this policy may result in disciplinary action, up to and including termination of employment.

B. All suspected violations will be reviewed by the Information Technology Department in coordination with the Department of People and Culture, and when necessary, other relevant City departments. The City reserves the right to audit email activity to ensure policy compliance.

Related Information:

The Department of Information Technology is responsible for publishing procedures related to the ongoing management of this policy. Email management procedures will include but are not limited to email account retention, exception procedures, and account deletion timelines.

Related Policies:

Information and Systems Security Policy
Laptop Computer and Mobile Device Policy
Remote Access Virtual Private Network (VPN) Security Policy
Electronic Signatures
Artificial Intelligence (AI) Policy

Other Related Information:

City of Providence Technology Password Guidelines