Email Policy

1.0 Purpose

Electronic mail (email) is a primary communication tool essential for business operations within the organization. However, its misuse can create significant legal, privacy, security, and reputational risks. The purpose of this policy is to ensure the appropriate, secure, and lawful use of the organization's email system. It defines acceptable and unacceptable uses and clarifies user responsibilities regarding email security, content, and retention.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, agents, and any other individual ("Users") granted access to the organization's email system. It covers all email sent from or received by an organization-provided email address (@\[organization_domain].com) and the use of organizational email services on any device.

3.0 Policy Statements

3.1 General Use and Expectations

*   **Business Purpose:** The organization's email system is provided primarily for conducting official organizational business.
*   **Limited Personal Use:** Limited, occasional personal use may be permissible provided it does not interfere with job performance, consume significant resources, violate any organizational policies (including the Acceptable Use Policy), or incur costs for the organization. Users should have no expectation of privacy in their use of the organization's email system.
*   **Monitoring:** Use of the organization's email system is subject to monitoring, logging, and review by authorized personnel for security, compliance, and operational purposes, in accordance with applicable laws and organizational policies.

3.2 Security Practices

*   **Account Security:** Users are responsible for safeguarding their email account credentials (passwords) according to the organization's Password Policy. Sharing email account access is prohibited.
*   **Malicious Content:** Users must exercise extreme caution when handling emails from unknown or unverified senders. Do not open unexpected attachments, click suspicious links, or provide sensitive information in response to unsolicited emails. Report suspicious emails (phishing attempts, spam, malware) immediately to the IT Help Desk or designated security contact.
*   **Sending Sensitive Information:** Sending sensitive or confidential organizational data (as defined by the Data Classification Policy) via email requires adherence to the Data Protection Standard, which may include requirements for encryption or use of approved secure file transfer

methods. Avoid sending sensitive data via email unless absolutely necessary and appropriately protected.

3.3 Unacceptable Use

The organization's email system must not be used for activities that violate the law, organizational policies, or ethical standards. Such activities are detailed in the Acceptable Use Policy and include, but are not limited to:

* Sending spam, chain letters, or unauthorized bulk emails.
* Transmitting offensive, harassing, discriminatory, defamatory, or threatening content.
* Distributing malicious software (viruses, worms, etc.).
* Violating copyright or intellectual property laws.
* Engaging in illegal activities or fraudulent schemes.
* Forging email headers or attempting to impersonate others.
* Using email for unauthorized commercial solicitation or outside business activities.

3.4 Representation and Disclaimers

* When sending emails externally, users represent the organization. Ensure communications are professional and appropriate.
* When expressing personal opinions that might be construed as representing the organization, include a disclaimer stating that the views expressed are personal and not necessarily those of the organization (as detailed in the Acceptable Use Policy).

3.5 Email Retention and Business Records

* Email messages should only be retained if they qualify as an official organizational business record needed for legitimate and ongoing business, legal, or regulatory purposes.
* Emails identified as business records must be retained and disposed of according to the official organizational Record Retention Schedule and related policies/procedures. Users may be required to file such emails in designated record-keeping systems.
* Non-record emails (e.g., transitory messages, personal communications) should be deleted regularly to manage mailbox size and reduce data clutter.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods. These may include monitoring email system usage logs, content filtering, audits (internal and external), investigation of reported incidents, and review of security tool reports.

4.2 Exceptions

Any exception to this policy requires formal, documented justification and advance approval from the designated IT authority (e.g., Precision Computer team or Information Security).

4.3 Enforcement

Violation of this policy may lead to disciplinary action, up to and including termination of employment or contract, suspension or revocation of email access, and potential legal action, depending on the severity of the violation.

5.0 Related Policies

Users should familiarize themselves with the following related organizational documents:

* Acceptable Use Policy (AUP)
* Password Policy
* Data Classification Policy
* Data Protection Standard
* Record Retention Schedule / Policy
* Information Security Policy (Overall)
* Social Media Policy (regarding communication standards)

Revision #2
Created 28 August 2024 16:51:22 by Daniel O
Updated 16 September 2025 22:10:08 by Travis Woolery