Acceptable Use Policy

1.0 Purpose

This policy outlines the acceptable use of the organization's information technology resources. Its purpose is to ensure these resources are used for legitimate business purposes, to protect employees, partners, and the organization from illegal, damaging, or unethical actions conducted knowingly or unknowingly via these resources, and to safeguard the confidentiality, integrity, and availability of information systems. The organization is committed to a culture of openness, trust, and integrity, and this policy supports these values by defining clear expectations for responsible use. Effective security is a shared responsibility, requiring the participation and support of every user.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, agents, and other workers of the organization and its subsidiaries ("Users"). It governs the use of all information, electronic and computing devices, network resources, and systems (including internet, intranet, extranet, email, and cloud services) owned, leased, or managed by the organization, as well as personal or third-party devices when used to conduct organization business or interact with internal networks and business systems.

3.0 Policy Statements

3.1 Ownership and General Use

* All organization-provided IT resources, including computer equipment, software, operating systems, storage media, network accounts, and associated data, are the property of the organization.
* These systems are intended primarily for business purposes in service of the organization's interests and its clients/customers. Limited personal use may be permissible provided it is brief, occasional, does not interfere with work duties, does not consume significant resources, and complies with all organizational policies (including this AUP). Users should have no expectation of privacy when using organizational resources. Refer to Human Resources policies for further details on personal use expectations.
* Users are responsible for exercising good judgment and conducting their activities in accordance with organizational policies, standards, and applicable laws and regulations.

3.2 Security Requirements

* Users must comply with the organization's Password Policy for all system and user-level passwords. Sharing passwords or allowing others (including family members) to use your account is strictly prohibited.

* All computing devices used to access organizational resources must comply with the Minimum Access Policy and relevant workstation security standards.
* Workstations must be secured (screen locked or logged off) when unattended. Password-protected screensavers with an automatic activation of 10 minutes or less are required.
* Users must exercise extreme caution when handling emails or files from unknown senders or unverified sources, particularly regarding opening attachments or clicking links that could contain malware.
* Providing unauthorized access to organizational resources, either deliberately or through failure to secure credentials or devices, is prohibited.

3.3 Proprietary and Confidential Information

* Users must handle proprietary and confidential organizational information appropriately, adhering to the Data Classification Policy and Data Protection Standard.
* When posting to external forums (newsgroups, etc.) from an organizational email address or identifying oneself as affiliated with the organization, users must include a disclaimer stating that the opinions expressed are their own and not necessarily those of the organization, unless the posting is an official duty.
* Providing information about or lists of organizational employees to external parties without authorization is prohibited.

3.4 Unacceptable System and Network Activities

The following activities are strictly prohibited:

* Engaging in any activity that is illegal under local, state, federal, or international law.
* Violating intellectual property rights (copyright, patent, trade secret), including installing or distributing unlicensed ("pirated") software, or unauthorized copying/distribution of copyrighted materials (music, images, text, etc.).
* Introducing malicious software (viruses, worms, Trojan horses, ransomware, spyware) into the network.
* Attempting or effecting security breaches or disruptions:
    * Unauthorized access to data, servers, or accounts.
    * Network sniffing, port scanning, security scanning, packet spoofing, denial-of-service attacks, ping floods, or forging routing information without explicit authorization from the designated IT authority (e.g., Precision Computer).
    * Circumventing user authentication or security measures of any host, network, or account.
    * Monitoring network data not intended for the user's device unless explicitly authorized as part of job duties.
    * Interfering with or denying service to any user or system.
    * Using programs/scripts/commands intended to interfere with or disable another user's session.
* Introducing honeypots, honeynets, or similar unauthorized security-testing technologies onto the network.
* Exporting software or technical information in violation of export control laws. Consult management if unsure.

3.5 Unacceptable Email and Communication Activities

The following activities are strictly prohibited:

* Sending unsolicited bulk email ("spam"), junk mail, chain letters, "Ponzi" or pyramid schemes.
* Engaging in harassment via email, messaging, or other communication channels (based on language, frequency, or message size).
* Unauthorized use or forgery of email header information.
* Soliciting email for addresses other than one's own with intent to harass or collect replies fraudulently.
* Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).
* Using organizational resources to procure or transmit material that violates sexual harassment or hostile workplace laws.
* Making fraudulent offers or unauthorized statements about warranties.

3.6 Blogging and Social Media

* All activities on blogs, wikis, social networking sites, and related platforms are subject to this AUP, whether using organizational or personal systems, if the activity relates to the organization or identifies the user as affiliated with it. Refer to the organization's Social Media Policy for detailed guidance.
* Users must not disclose organizational confidential or proprietary information or trade secrets.
* Users must not engage in blogging or social media activities that could harm the organization's reputation or goodwill, or that involve discriminatory, disparaging, defamatory, or harassing content prohibited by other organizational policies (e.g., Non-Discrimination and Anti-Harassment).
* Users must not attribute personal statements, opinions, or beliefs to the organization. If expressing personal opinions while identifying affiliation, clearly state that the views are personal.
* Organizational trademarks, logos, or other intellectual property may not be used in personal blogging or social media activities without authorization.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team) will verify compliance with this policy through various methods, including but not limited to, monitoring network traffic, reviewing system logs, audits (internal and external), inspection of devices, and analysis of reports from security tools. User activity on organizational resources may be monitored without notice.

4.2 Exceptions

Certain restrictions (e.g., security scanning, network monitoring) may be exempted for specific job responsibilities (e.g., IT system administration) with appropriate authorization. Any other exception to this policy requires formal, documented justification and advance approval from the designated IT authority (e.g., Precision Computer team).

4.3 Enforcement

Violation of this policy may result in disciplinary action, up to and including termination of employment or contract, as well as potential legal action. Access privileges may be restricted or revoked pending investigation.

5.0 Related Policies and Definitions

* **Related Policies:**
  * Data Classification Policy
  * Data Protection Standard
  * Human Resources Policies (regarding personal use, conduct)
  * Minimum Access Policy
  * Non-Discrimination and Anti-Harassment Policy
  * Password Policy
  * Social Media Policy
  * Workstation Security Policy/Standards
* **Definitions:**
  * **Blogging:** Writing and publishing posts on a blog (web log).
  * **Honeypot/Honeynet:** Decoy computer systems set up to attract and detect unauthorized use attempts or malware.
  * **Proprietary Information:** Information owned by the organization, often confidential, providing a competitive advantage (e.g., trade secrets, internal processes, customer lists).
  * **Spam:** Unsolicited bulk electronic messages, typically commercial emails.

Revision #2
Created 28 August 2024 16:48:13 by Daniel O
Updated 16 September 2025 22:10:08 by Travis Woolery