Acceptable Use Policy

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and systems at <Company Name>. Acceptable use requirements are designed to safeguard sensitive <Company Name> customer data, and to protect the company and its employees. Inappropriate use may expose <Company Name> to legal issues, cyber attacks and breaches, and other risks.

Scope

This policy applies to the use of all company-provided IT resources, regardless of their geographic location, and to all <Company Name> employees and contractors.

Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

Policy Statement

<Company Name> assets are primarily intended for business purposes. Users are responsible for exercising good judgment regarding appropriate personal use of company resources, such that this use does not negatively impact <Company Name> in any way.

Acceptable Use

The Acceptable Use Policy outlines the acceptable use of computer equipment and systems at the company.

General Use

General Use and Ownership

<Company Name> proprietary and confidential information stored on electronic and computing devices remains the sole property of <Company Name>, whether the devices themselves are owned by .<Company Name>, an employee, or a third party.
Theft, loss, or unauthorized disclosure of <Company Name> proprietary and confidential information must be promptly reported.

Access, use, or sharing of <Company Name> proprietary information is allowed only to the extent it is both authorized and necessary to fulfill the employee's assigned job duties.
Good judgment must be exercised regarding the reasonableness of personal use of company-provided equipment.
Software must be properly licensed, free of malicious code, and authorized, before it is installed on company owned or managed assets.

Security and Proprietary Information

System and individual user passwords must comply with the Authentication and Password Policy.
Providing one's personal access credentials to another individual, either deliberately or through failure to secure its access, is prohibited. Passwords for individual accounts may not be shared.
Employees are required to secure equipment and log out of or lock systems when leaving them unattended for any period of time.
All computing devices must be configured such that their use requires entering a password after at most 15 minutes of inactivity.
Employees must use extreme caution when opening email attachments, particularly those received from unknown senders, as any attachment may contain malware.
Employees must encrypt their devices if asked, and must not interfere with or reduce the level of encryption on their devices.
Employees should install operating system security updates onto their devices if asked to do so, or if prompted by the system's automatic updates feature. Employees should also be proactive about applying system security updates to their devices.
Employees must be mindful of sensitive information, whether on paper or in electronic form. Ii
Sensitive information must be secured when left unattended, and kept out of sight when visitors are present.
Electronic media and papers that contain sensitive data must be sanitized or destroyed as soon as that data is no longer needed.

Prohibited use

The following activities and actions are prohibited.

Using <Company Name> information assets in any way that violates international, federal, state, or local law or regulations or violates any <Company Name> policy or procedure.
Accessing data by logging into a server or account that one is not explicitly authorized to access, or accessing data in excess of one's authority.
Copying, moving, or storing sensitive customer information without a strong business need.
Sharing individual user credentials (passwords, private keys, etc.)
Sharing team or group credentials outside the authorized scope of the team or group.
Unauthorized disclosure, release, or transmission of any company data.
Downloading, storing, duplicating, distributing, printing, or otherwise using copyrighted, patented, or trademarked material from any source (including both published works as well as the internet) without the owner's permission.

Taking actions that are intended to breach, or may result in a breach, of <Company Name> or any other company's or individual's security, confidentiality or privacy. These actions include (but are not limited to):

Taking actions intended to capture information to which the user is not authorized (such as keystroke logging, network sniffing, network mapping, port scanning or vulnerability scanning).

Circumventing, misusing, or exceeding any authentication, privilege, or security mechanism.

Impersonating any person or entity or falsely stating or otherwise misrepresenting affiliation with a person or entity.

Interfering with or denying service to any authorized user or process.

Taking actions meant to disrupt, trick, circumvent, or hide disallowed actions, including (but not limited to) flooding, spoofing, forging data, or causing a denial of service.

Writing, modifying or distributing computer viruses, Trojan horses, worms, or any other form of malicious software.

Taking any action for malicious purposes, or in any manner negatively impacting the interests of the company.

Assisting others in activities which violate this or other <Company Name> policies and standards, or authorizing others to perform such activities.

Introducing honeypots, honeynets, or similar technology to company resources, unless explicitly authorized as part of <Company Name>'s security program.