Acceptable Use Policy

Purpose

[redacted], a partner of [redacted], is committed to securing company data and customer information, including Customer Proprietary Network Information (CPNI). This policy is intended to guide [redacted] employees in avoiding unauthorized activities when accessing company assets and information.

End-users accessing networks related to [redacted] or [redacted] are expected to protect data access points and ensure the confidentiality, integrity, and availability of [redacted]' network resources.

Employees must access information solely for business-related purposes. For example, they should use company-provided equipment only to access the intranet and log usage records. Usage on [redacted] systems may be monitored and referenced in cases of suspected illegal activity.

Any employee who observes unethical or suspicious behavior when using company systems should document the activity and report it to the [redacted] team promptly.

Examples of Unacceptable Use

1. **Compromised Personal Information**
   [redacted] takes extensive measures to protect customer information, including using secure, encrypted databases and employee activity logs. If customer information is compromised, the security team will initiate immediate response measures, including reviewing logs to investigate any illicit activity.
2. **Preventive Actions**
   Employees who misuse the [redacted] network and fall victim to identity theft or fraudulent activities due to negligent actions are solely responsible for initiating their own resolutions.
3. **Unlawful Acts by Employees**
   Misuse of company assets can harm both [redacted] and its customers. Legal action will be pursued against employees found responsible for asset misuse following thorough investigation and resolution.
4. **Failure to Report Misconduct**
   Employees aware of unethical or suspicious activities but who fail to report such behavior will be subject to investigation and potential prosecution for neglecting to take appropriate action. Reports should be filed with the [redacted] team to enable corrective measures against system misuse.

PDF-XChange Editor Click to BUY NOW! www.pdf-xchange.com

Email Use Policy

[redacted] requires that all email usage complies with the following standards:

1. **Professional Use**
   Employees must use the [redacted] email system professionally, ethically, and lawfully. Emails should be limited to work-related matters and not used for personal communication. All email use must adhere to the [redacted] Standards of Conduct.
2. **Privacy Expectation**
   Employees should have no expectation of privacy when using the [redacted] email system. All emails can be monitored at any time, and emails sent or received are property of [redacted].
3. **Consent to Monitoring**
   By using [redacted] systems and hardware, employees consent to email monitoring, access, review, reproduction, and deletion. If an employee is identified as a potential security risk, their device may be subject to a full email wipe or, in extreme cases, a complete device wipe. Email data created, received, transmitted, or stored on [redacted] systems may be inspected, disclosed, and managed as outlined in this policy.
4. **Encryption of Sensitive Information**
   All emails containing sensitive information, such as Personally Identifiable Information (PII) or financial data, must be encrypted. The system owner is responsible for implementing administrative controls to detect and prevent the transmission of unencrypted protected information outside the internal network. Any incidents involving unencrypted protected information will be logged, and the employee responsible will be notified.