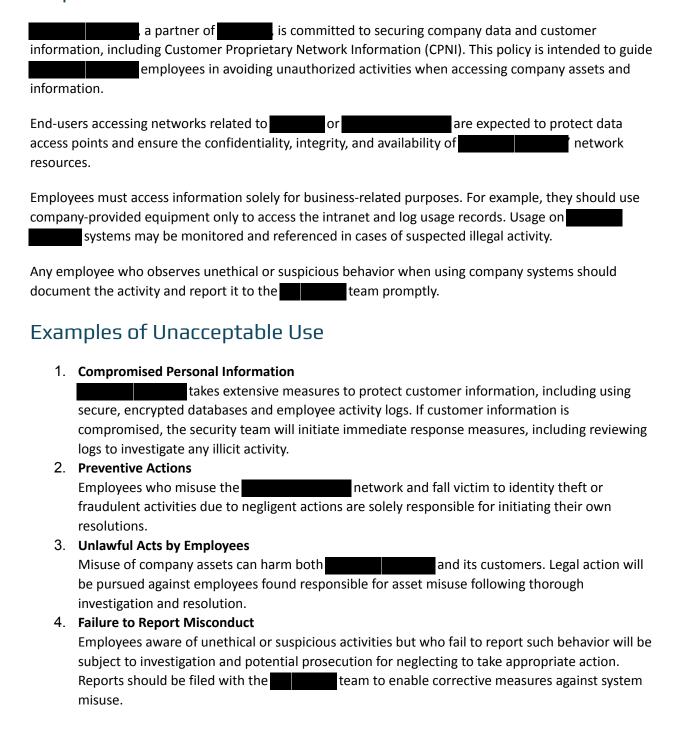




Acceptable Use Policy

Purpose







Email Use Policy

requires that all email usage complies with the following standards: 1. Professional Use Employees must use the 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 Standards of Conduct. 2. Privacy Expectation Employees should have no expectation of privacy when using the email system. All emails can be monitored at any time, and emails sent or received are property of 3. Consent to Monitoring By using 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 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

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.