

- f. [Insert Company name] will install anti-virus software on all workstations to prevent transmission of malicious software. This anti-virus software is regularly updated.
- g. Portable workstations are also subject to the same safeguards and protections.
- h. Portable workstations are maintained in a safe and secure manner when transported.
- i. Any portable device that contains sensitive and regulated data must be encrypted.
 - i. Portable media is also subject to the same requirements.
- j. Networks are secured with a Firewall.
- k. Network access is limited to legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.
- l. Firewall console and other management ports are appropriately secured or disabled and are in a physically secure environment.
- m. Mechanisms to log failed access attempts are in place.
 - i. [Insert Company name] will lock accounts after [3] failed login attempts. (Each organization must choose the number of failed login attempts based on its risk analysis.)
- n. The configuration of firewalls used to protect networks is approved by the Security Officer or designee and maintained by the IT Department.
- o. Firewalls will be maintained as staff change positions.
- p. Servers are located in a physically secure environment and are on a secure network with firewall protection.
- q. The system administrator or root account is password protected.
- r. A security patch and update procedure are established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
- s. All unused or unnecessary services are disabled.

Violations:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Violation may also result in civil and criminal penalties to [Insert Company name] as determined by federal and state laws and regulations related to loss of data.

Attachments: None

Related Policies: None