

Network Security Policy

1. Overview: The Company wishes to provide a secure network infrastructure in order to protect the integrity of corporate data and mitigate risk of a security incident. The purpose of this policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure. However, this policy purposely avoids being overly specific in order to provide some latitude in implementation and management strategies.

2. Scope: This policy covers all IT systems and non-end user devices that comprise the corporate network or that are otherwise controlled by the Company.

3. Policy

3.1 Network Device Passwords: A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches, and servers, must be held to higher standards than standard user-level or desktop system passwords.

Password Construction

The following statements apply to the construction of passwords for network devices:

- Passwords should be at least 10 characters
- Passwords should be comprised of a mix of upper and lower case letters, numbers and special characters (punctuation marks and symbols)
- Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary
- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
- Passwords should not include "guessable" data such as personal information like birthdays, addresses, phone numbers, locations, etc.

Failed Logons

In order to guard against password-guessing and brute-force attempts, the Company must lock a user's account after 3 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the IT Director.

In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

Change Requirements

Passwords must be changed according to the Company's Password Policy. Additionally, the following requirements apply to changing network-device passwords:

- If any network device password is suspected to have been compromised, all network device passwords must be changed immediately.
- If a company network or system administrator leaves the Company, all passwords to which the administrator could have had access must be changed immediately. This statement also applies to any consultant or contractor who has access to administrative passwords.
- Vendor default passwords must be changed when new devices are put into service.

Administrative Password Guidelines

Generally, administrative (also known as "root") access to systems should be limited to only those who have a legitimate business need for this type of access. Additionally, administrative access to network devices should be logged.

3.2 Logging: The logging of certain events is an important component of good network management practices. A member of the Company's IT team should review the logs as frequently as is reasonable. Logs should be retained in accordance with the Company's Retention Policy. Unless otherwise determined by the IT Director, logs should be considered operational data. Logging needs vary depending on the type of network system, and the type of data the system holds.

Application Servers

Examples: Web, email, database servers

Requirement: Logging of at least errors, faults, and login failures is encouraged but not required. No passwords should be contained in logs.

Network Devices

Examples: Firewalls, network switches, routers

Requirement: Logging of at least errors, faults, and login failures is encouraged but not required. No passwords should be contained in logs.

Critical Devices

Examples: File servers, lab or manufacturing machines, systems storing intellectual property.

Requirements: Logging of errors, faults, and login failures is encouraged but not required. No passwords should be contained in logs.

3.3 Firewalls: Firewalls are arguably the most important component of a sound security strategy. Internet connections and other unsecured networks must be separated from the Company network through the use of a firewall. The following statements apply to the Company's implementation of firewall technology:

- Firewalls must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.

- No unnecessary services or applications should be enabled on firewalls. The Company should use 'hardened' systems for firewall platforms, or appliances.
- Clocks on firewalls should be synchronized with the Company's other networking hardware using Network Time Protocol (NTP) or another means. Among other benefits, this will aid in problem resolution and security incident investigation.
- The firewall ruleset must be documented and audited annually. Audits must cover each rule, what it is for, if it is still necessary, and if it can be improved.
- For its own protection, the firewall ruleset should include a "stealth rule," which forbids connections to the firewall itself.
- The firewall should log dropped or rejected packets.

3.4 Networking Hardware:

Networking hardware, such as routers, switches, hubs, bridges, and access points, should be implemented in a consistent manner. The following statements apply to the Company's implementation of networking hardware:

- Networking hardware must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.
- Clocks on all network hardware should be synchronized using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.
- If possible for the application, switches are preferred over hubs. When using switches the Company should use Virtual Local Area Networks (VLANs) to separate networks if it is reasonable and possible to do so.
- Access control lists should be considered on network devices that prohibit direct connections to the devices. Exceptions to this are management connections that can be limited to known sources.
- The Company should consider disabling unused services and ports on networking hardware.
- The Company should consider restricting access to the administrative ports of networking hardware with a firewall or access control list.

3.5 Network Servers: Servers typically accept connections from a number of sources, both internal and external. Generally, the more sources that connect to a system, the more risk that is associated with that system, so it is particularly important to secure network servers. The following statements apply to the Company's use of network servers:

- Unnecessary files, services, and ports should be removed or blocked. If possible, follow a server-hardening guide, which is available from the leading operating system manufacturers.
- Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.

- If possible, a standard installation process should be developed for the Company's network servers. This will provide consistency across servers no matter what employee or contractor handles the installation.
- Clocks on network servers should be synchronized with the Company's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

3.6 Intrusion Detection/Intrusion Prevention: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology can be useful in network monitoring and security. The tools differ in that an IDS alerts to suspicious activity whereas an IPS blocks the activity. When tuned correctly, IDSs are useful but can generate a large amount of data that must be evaluated for the system to be of any use. IPSs automatically take action when they see suspicious events, which can be both good and bad, since legitimate network traffic can be blocked along with malicious traffic.

The Company neither requires nor prohibits the use of IDS or IPS systems. The decision to use IDS/IPS systems is left to the discretion of the IT Director.

3.7 Security Testing: Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining the Company's network security.

Internal Security Testing

Internal security testing is allowable, but only by employees whose job functions are to assess security, and only with permission of the IT Director. Internal testing should have no measurable negative impact on the Company's systems or network performance.

External Security Testing

The Company encourages external security testing, but does not provide rigid guidelines regarding at what intervals the testing should occur. Testing should be performed as often as is necessary, as determined by the IT Director or the Senior Leadership Team. External testing must not negatively affect network performance during business hours or network security at any time. As a rule, "penetration testing," which is the active exploitation of company vulnerabilities, should be discouraged. If penetration testing is performed, it should be performed under limited circumstances and in a way that limits the negative affect on company systems and data.

3.8 Disposal of Information Technology Assets: IT assets, such as network servers and routers, often contain sensitive data about the Company's network communications. When such assets are decommissioned, the following guidelines must be followed:

- Any asset tags or stickers that identify the Company must be removed before disposal.
- Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.

- At a minimum, data wiping must be used. Simply reformatting a drive or deleting data does not make the data unrecoverable. If wiping is used, the Company must use the most secure commercially-available methods for data wiping. Alternatively, the Company has the option of physically destroying the data storage mechanism from the device (such as its hard drive or solid state memory).

3.9 Network Compartmentalization: Good network design is integral to network security. The Company requires the following with regard to network compartmentalization:

Higher Risk

Examples: Guest network, wireless network

Requirements: Segmentation of higher risk networks from the Company's internal network is encouraged but not required.

Externally Accessible Systems

Examples: Email servers, web servers

Requirements: Segmentation of externally-accessible systems from the Company's internal network is encouraged but not required.

Internal Networks

Examples: Sales, Finance, Human Resources.

Requirements: Segmentation of internal networks from one another can improve security as well as reduce chances that a user will access data that he or she has no right to access. The Company encourages, but does not require, such segmentation.

3.10 Network Documentation: The Company requires that network documentation be performed and updated on a yearly basis. At a minimum, network documentation must include:

- Network diagram(s)
- System configurations
- Firewall ruleset
- IP Addresses Access Control Lists

3.11 Antivirus/Anti-Malware: The Company provides the following guidelines on the use of antivirus/anti-malware software:

- All company-provided user workstations must have antivirus/anti-malware software installed.
- Workstation software must maintain a current "subscription" to receive patches and virus signature/definition file updates.
- Patches, updates, and antivirus signature file updates must be installed in a timely manner, either automatically or manually.

3.12 Software Use Policy: The Company provides the following requirements for the use of software applications:

- Only legally licensed software may be used. Licenses for the Company's software must be stored in a secure location.
- Open source and/or public domain software can only be used with the permission of the IT Director.
- Software should be kept reasonably up-to-date by installing new patches and releases from the manufacturer.
- Vulnerability alerts should be monitored for all software products that the Company uses.

3.13 Maintenance Windows and Scheduled Downtime: Certain tasks require that network devices be taken offline, either for a simple reboot, an upgrade, or other maintenance. When this occurs, the IT Staff should make every effort to perform the tasks at times when they will have the least impact on network users, and any downtime will be scheduled with, and communicated to, the affected parties. See also the IT Change Management Policy.

3.14 Change Management: The IT Staff must document hardware and/or configuration changes to network devices in a "change log." Network devices must bear a sticker or tag indicating essential information, such as the device name, IP address, Mac address, asset information, and any additional data that may be helpful, such as information about cabling.

3.15 Suspected Security Incidents: When a security incident is suspected that may affect a network device, the IT Staff should refer to the Company's Incident Response policy for guidance.

3.16 Redundancy: The Company wishes to provide the IT Director with latitude to determine the appropriate level of redundancy for critical systems and network devices. Redundancy should be implemented where it is needed, and should include some or all of the following:

- Hard drive redundancy, such as mirroring or RAID
- Server level redundancy, such as clustering or high availability
- Component level redundancy, such as redundant power supplies or redundant NICs
- Keeping hot or cold spares onsite

3.17 Manufacturer-Support Contracts: When purchasing critical hardware or software, the Company should consider purchasing a maintenance plan, support agreement, or software subscription that will allow the Company to receive updates to the software and/or firmware for a specified period of time. If such a plan is purchased, it should meet the following standards: Hardware: The arrangement should allow for repair/replacement of the device within an acceptable time period, as determined by the

IT Director, as well as firmware or embedded software updates. Software: The arrangement should allow for updates, upgrades, and hotfixes for a specified period of time.

3.18 Security-Policy Compliance: It is the Company's intention to comply with this policy not just on paper but in its everyday processes as well. With that goal in mind, the Company requires the following:

Security-Program Manager

An employee must be designated as a manager for the Company's security program. He or she will be responsible for the Company's compliance with this security policy and any applicable security regulations. This employee must be responsible for (i) the initial implementation of the security policies, (ii) ensuring that the policies are disseminated to employees, (iii) training and retraining of employees on the Company's information security program (as detailed below), (iv) any ongoing testing or analysis of the Company's security in compliance with this policy, (v) updating the policy as needed to adhere with applicable regulations and the changing information security landscape.

Security Training

A training program must be implemented that will detail the Company's information security program to all users and/or employees covered by the policy, as well as the importance of data security. Employees must sign off on the receipt of, and in agreement to, the user-oriented policies. Re-training should be performed at least annually.

Security-Policy Review

The Company's security policies should be reviewed at least annually. Additionally, the policies should be reviewed when there is an information security incident, or a material change to the Company's security policies. As part of this evaluation the Company should review:

- Any applicable regulations for changes that would affect the Company's compliance or the effectiveness of any deployed security controls.
- If the Company's deployed security controls are still capable of performing their intended functions.
- If technology or other changes may have an effect on the Company's security strategy.
- If any changes need to be made to accommodate future IT security needs.