Network Security Policy

Contents

1. Overview 3
2. Purpose 3
3. Policy 3
   3.1. Authorized Personnel 3
   3.2. Network Device Passwords 3
   3.3. Password Construction 3
   3.4. Failed Logons 4
   3.5. Change Requirements 4
   3.6. Password Policy Enforcement 4
   3.7. Administrative Password Guidelines 4
4. Logging 5
   4.1. Application Servers 5
   4.2. Network Devices 5
   4.3. Critical Devices 5
   4.4. Log Review 5
   4.5. Log Retention 5
5. Firewalls 5
   5.1. Configuration 5
   5.2. Outbound Traffic Filtering 6
   5.3. Data Leakage Controls 6
6. Networking Hardware 6
   6.1. Hardening Standards 6
   6.2. Network Servers 7
7. Intrusion Detection/Intrusion Prevention 7
8. Data Loss Prevention Technologies 7
9. Security Testing 7
   9.1. Internal Security Testing 8
   9.2. External Security Testing 8
10. Disposal of Information Technology Assets 8
11. Network Compartmentalization & Reduced Exposure 8
12. Network Documentation 8

1. Overview

The Remington Group maintains a secure network infrastructure through the following enumerated policies in order to protect the integrity and confidentiality of client and Remington Group data and mitigate the risk of a security incident.

2. Purpose

The purpose of this policy is to establish the guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support Remington Group's comprehensive set of security policies. This policy covers all IT systems and devices that comprise the Remington Group network or that are otherwise controlled by Remington Group personnel directly or through third parties.

3. Policy

3.1. Authorized Personnel

The creation and management of all accounts, including system and user accounts, must be authorized in advance in writing by the CIO in consultation with the Remington Group's contracted IT support personnel.
Access and maintenance of applications systems, network components (including routers, firewalls, voice communications servers, voice recording servers, etc.), operating systems, virtualization components, hypervisors, or other information objects is restricted to authorized personnel only.

Access to and maintenance of applications, systems, network components (including routers, firewalls, voice communications servers, voice recording servers, etc.), operating systems, virtualization components, hypervisors, or other information objects shall be granted based upon job function.
Approval of the CIO is required prior to creating all user and privileged accounts (e.g., system or security administrator).

Privileged accounts (e.g., system or security administrator) must be logged and reviewed on at least a quarterly basis.

Inactive user and privileged accounts (e.g., system administrator or security administrator) will be disabled or locked after 15 days or less.

3.2. Network Device Passwords

Default system accounts (e.g., guest, administrator) will always be disabled or renamed upon initial system builds. Local account credentials not be handed over to users and it will be keep within IT department for service perspective.

3.3. Password Construction

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

- Passwords must be at least twelve characters.
- Passwords must be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols), including a mix of upper and lowercase characters.
- Passwords must not be comprised of an obvious keyboard sequence (i.e., QWERTY).
- Passwords must not include "guessable" data such as personal information like birthdays, addresses, Remington Group public information, phone numbers, locations, etc.

3.4. Failed Logons

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account.

In order to guard against password-guessing and brute-force attempts, the Remington Group' s IT Department will lock a user's account after 5 unsuccessful logins. The locked account shall remain locked for a minimum duration of on hour or until the IT Department manually resets and unlocks the account via personal support request of the user.

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**."

3.5. Change Requirements

User and privileged account (e.g., system or security administrator) passwords, with the exception of the Domain Administrator password and passwords used in conjunction with Windows services, must be changed at least every 90 days by enforcement of group policies. In order to mitigate any security risk associated with the Domain Administrator account and any accounts used for Windows services, the following will be implemented:

- The Domain Administrator password has been changed to a highly complex password and is stored in a locked cabinet to which only the Remington Group' s IT DepartmentAdministrators have access to.
- All users requiring privileged account (e.g., system or security administrator access) have been provided with separate administrative credentials.
- Where feasible, any account used in conjunction with a Windows service has been denied the right to logon locally or through Terminal Services through theimplementation of Group Policies.
- 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 promptly.
- If a Remington Group network or system administrator leaves the Firm, all passwords to which the administrator could have had access must be changed promptly. This statement also applies to any consultant or contractor who has access to administrative passwords.

3.6. Password Policy Enforcement

Where passwords are used, an application must be implemented that enforces the Remington Group's password policies on construction, changes, re-use, lockout, etc.

3.7. Administrative Password Guidelines

As a rule, 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.
This is particularly important for network devices, since administrative changes can have a major effect on the network, and, as such, network security. Additionally, administrative access to network devices should be logged.

4. Logging

The following sections detail the Remington Group's requirements for logging and log review.

4.1. Application Servers

Logs from application servers are of interest since these servers often allow connections from a large number of internal and/or external sources. These devices are often integral to smooth business operations.

Examples: Web, email, database servers.

Requirement: Errors, faults, and login failures will be logged. No passwords should be contained in logs.

4.2. Network Devices

Logs from network devices are of interest since these devices control all network traffic, and can have a huge impact on the Remington Group's network security.

Examples: Firewalls, network switches, routers

Requirement: Errors, faults, and login failures will be logged. No passwords should be contained in logs.

4.3. Critical Devices

Critical devices are any systems that are critically important to business operations. These systems may also fall under other categories above. In any cases where this occurs, this section shall supersede.

Examples: File servers, JIM2 Servers, PrintPoint Server or manufacturing machines (BizPrint), systems storing intellectual property

Requirements: Errors, faults, and login failures will be logged. No passwords should be contained in logs.

4.4. Log Review

The CIO and/or the Remington Group’s Network Administrator, as appropriate, will review the logs at least once per month.

4.5. Log Retention

Audit logs may be modified or deleted only upon the approval of the Remington Group's CIO and/or the Remington Group's Network Administrator. Production system audit logs must be retained for a minimum of 6 months.

5. Firewalls

Firewalls are one of the most important components of the Remington Group's security strategy. Internet & MPLS Network connections and other unsecured networks must be separated from the Remington Group network through the use of a firewall

5.1. Configuration

The following statements apply to the Firm'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 Remington Group should use 'hardened' systems for firewall platforms, or appliances.
- Clocks on firewalls should be synchronized with the Remington Group's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.
- All firewall rules must be reviewed annually and approved by the CIO in concert with the Remington Group's Network Administrator.
- All firewall and router rules must be reviewed at least annually. Audits must cover each rule, what it is for, if it is still necessary, and if it can be improved.
- Changes to firewall rules must be logged and the logs must identify the administrator performing the change and when the change occurred.
- For its own protection, the firewall rule set must include a "stealth rule," which forbids connections to the firewall itself.
- The firewall must log dropped or rejected packets.

5.2. Outbound Traffic Filtering

Firewalls must be configured to filter outbound connections from the network. Blocking outbound traffic prevents users from accessing unnecessary or dangerous services. By specifying exactly what outbound traffic to allow, all other outbound traffic is blocked. This type of filtering would block root kits, viruses, ransomware, and other malicious tools if a host were to become compromised.

The Remington Group requires that permitted outbound traffic be limited to only known "good" services, which are the following ports: 21, 25, 53, 80, 110, 443, and 995. All other outbound traffic must be blocked at the firewall unless an exception is granted from the CIO.

All outbound connections (e.g., HTTP, HTTPS, FTP, and Telnet) must be authenticated by a proxy device. CIO's approval is required for the establishment of encrypted protocol communications that cannot be authenticated by a proxy device.

5.3. Data Leakage Controls

Data leakage controls (e.g., logging access to files and folders designated at confidential on shared drives, disabling the ability to use removable drives, disabling of unapproved CD/DVD burners and hard drives) will be established to ensure that confidential Remington Group's or client data can't be physically or electronically removed without management authorization.

6. Networking Hardware

The following policy statements apply to the Remington Group's implementation of networking hardware:

6.1. Hardening Standards

The Remington Group recognizes that certain steps must be taken to prepare new hardware and software for deployment.

- Platform hardening should be benchmarked against industry/vendor standards and best practices (e.g., SANS, VISA, NSA, etc.)
- Current security updates, patches and anti-virus definitions will be applied.
- Unused protocols and services must be disabled prior to deployment into production.
- Unneeded user accounts must be disabled and default accounts (e.g. Administrator, Guest etc.) should be renamed.
- Sample programs and scripts must be deleted.
- Password parameters must be reconfigured to comply with Remington Group standards set forth in this policy.
- Logging and audit trails must be activated.

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. This requirement will aid in problem resolution and security incident investigation.
The Remington Group will restrict access to the administrative ports of networking hardware with a firewall or access control list.

6.2. Network Servers

The following statements apply to the Remington Group's network servers:

- Unnecessary files, services, and ports will be removed or blocked.
- Network servers, even those meant to accept public connections, must be protected by a firewall or

access control list.

- A standard installation process will be developed for the Remington Group's network servers.
- Clocks on network servers should be synchronized with the Remington Group's other networking hardware using NTP or another means. This will aid in problem resolution and security incident investigation

7. Intrusion Detection/Intrusion Prevention

The Remington Group requires the use of either a network intrusion detection system (NIDS) or a network intrusion protection system (NIPS) on critical or high-risk network segments.

The Remington Group will install a network intruder detection system (NIDS) or a network intruder prevention system (NIPS) to monitor all external network connections.

The network intruder detection systems (NIDS) or network intruder prevention systems (NIPS) will also monitor the internal network.

8. Data Loss Prevention Technologies.

Remington Group's clients who may provide personal or private information that requires extra care and protections against accidental disclosure or misuse.

As a result of this, the Remington Group will deployed technologies that will help protect sensitive information, (such as date of birth, social security number, etc…). These systems will generate alerts that will be monitored in real time to members of the Remington Group appointed by Remington Group administration. Every alert should be reviewed for accuracy and responded to accordingly.

9. Security Testing

The following sections detail the Remington Group's requirements for security testing.

- The Remington Group will conduct an annual internal and external vulnerability scan that encompasses all networks and hosts.
- The findings from vulnerability scans will be tracked and rescans will be performed until no findings are identified.

9.1. Internal Security Testing

Performance of internal security testing by members of the Remington Group's IT team is required annually. Internal security testing is allowable only with permission of the CIO in consultation with the firms contracted IT support personnel. Such testing must have no measurable negative impact on the Firm's systems or network performance.

9.2. External Security Testing

External security scans for known vulnerabilities and threats by a third party entity will be conducted quarterly.

10. Disposal of Information Technology Assets

IT assets, such as network servers and routers, often contain sensitive data about the Remington Group's network communications. When such assets are decommissioned, the following guidelines must be followed:

- Any asset tags or stickers that identify the Remington Group must be removed before disposal.
- Electronic media (e.g., tapes, disk drives, multifunction devices, copiers, etc.) will be destroyed by physical destruction.
- Destruction will be recorded in logs.

11. Network Compartmentalization & Reduced Exposure

Good network design is integral to network security. By implementing network compartmentalization, which is separating the network into different segments, the Remington Group will reduce its network-wide risk from an attack or virus outbreak. Further, security can be increased if traffic must traverse additional enforcement/inspection points.

Following a network best practice, all VOIP networks should be separated either physical or logically, by the use of vLANs, from the data network.

In order reduce the exposure of the network and possibly have unauthorized devices connect while being undetected, all physical data ports in the office space or conference rooms are to unplugged as to prohibit access. VOIP phones that have a data port are to be configured to have the data port disabled or the data ports configured for a non-usable configuration such as a “Blackhole vLAN”.

12. Network Documentation

Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network ensures that the Remington Group's IT Staff has a Remington Group understanding of the network architecture at any given time.

Network documentation should include:

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

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.

Only authorized individual of the Remington Group shall have access to any network diagrams. Therefore, all network diagrams and related documentation must be secured at all times. Unauthorized access to any Remington Group network documentation may result in disciplinary actions up to and including termination of employment

ACKNOWLEDGMENT

I have carefully read the Corporate Network Security Policy. I understand the contents, and I agree to comply with the said Policy.

Business Unit & Department			
Name			
Signature		Date	
Manager/Supervisor Signature		Date	