Security Policy

American Academy McAllister Institute of Funeral Service, Inc.

2019 version

Relationship of Parties

Priority Support Inc. (PSI), is an information technology consulting firm. PSI has serviced American Academy McAllister Institute of Funeral Service, Inc. (AAMI) (client) for several years under a standard Master Service Agreement and a Statement of Work. All terms in those documents are currently in effect. PSI follows industry best practices with regards to work done on behalf of client. PSI does not supply any developed software or operating systems. All hardware and software systems, as recommended by PSI are considered industry standard or by well-known long-standing companies. When possible PSI attempts to use domestic, US based companies.

Services Provided

PSI provides installation and/or management of the following items.

Network Equipment

User Access

Server Operating Systems

Back Ups and Disaster recovery

Employee training coordination

Penetration testing and monitoring

Network Security Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.
2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
3. The following services or features must be disabled:
    a. IP directed broadcasts
    b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
    c. TCP small services
    d. UDP small services
    e. All source routing and switching
    f. All web services running on router
    g. <Company Name> discovery protocol on Internet connected interfaces
    h. Telnet, FTP, and HTTP services
    i. Auto-configuration
4. The following services should be disabled unless a business justification is provided:
    a. Discovery protocols
    b. Dynamic trunking
    c. Scripting environments, such as the TCL shell
5. The following services must be configured:
    a. Password-encryption
    b. NTP configured to a corporate standard source
6. All routing updates shall be done using secure routing updates.

7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
9. Access control lists for transiting the device are to be added as business needs arise.
10. The router must be included in the corporate enterprise management system with a designated point of contact.
11. Each router must have the following statement presented for all forms of login whether remote or local:

    "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

12. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
13. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
14. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
    a. IP access list accounting
    b. Device logging

c. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
d. Router console and modem access must be restricted by additional security controls

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

User Accounts and Access Policies

Password Policies

All passwords must meet strong password requirements. Examples of such are as follows:

- At least 8 characters—the more characters, the better
- A mixture of both uppercase and lowercase letters
- A mixture of letters and numbers
- Inclusion of at least one special character, e.g., ! @ # ?]
  Note: do not use < or > in your password, as both can cause problems in Web browsers

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to client systems, are responsible for taking the appropriate steps to select and secure their passwords.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any

system that resides at any client facility, has access to the client network, or stores any non-public client information.

Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential information.

Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.

Do not use the "Remember Password" feature of applications (for example, web browsers).

Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Data Access Policies

All user accounts are created under direct approval of department heads only. New user account creation forms shall be signed before requesting creation.

Folder access permissions are granted only under direct approval of department heads. Folder access forms shall be specified and signed before any rights or access is granted.

Server Security Policy

All servers are actively monitored for security patch deployments and installation. Patches are applied either automatically or after a brief testing period depending upon the severity of a disruption due to an incompatible or failed patch installation. Any third-party patches not provided by the core operating system vendor follow this same approach.

Server administration accounts are used with minimum viable access rights. Domain admin users are not to be used on member servers.

The server security policy shall be as follows.

1. Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

2. Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by client. Effective implementation of this policy will minimize unauthorized access to proprietary information and technology.

3. Scope

All employees, contractors, consultants, temporary and other workers at Cisco and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by Cisco or registered under a Cisco-owned internal network domain.

This policy specifies requirements for equipment on the internal Cisco network. For secure configuration of equipment external to Cisco on the DMZ, see the Internet *DMZ Equipment Policy*.

4. Policy

4.1 General Requirements

4.1.1 All internal servers deployed at client must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec. The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures

4.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic.

4.2 Configuration Requirements

4.2.1 Operating System configuration should be in accordance with approved InfoSec guidelines.

4.2.2 Services and applications that will not be used must be disabled where practical.

4.2.3 Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

4.2.4 The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

4.2.5 Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

4.2.6 Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

4.2.7 If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

4.2.8 Servers should be physically located in an access-controlled environment.

4.2.9 Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3 Monitoring

4.3.1 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.

4.3.2 Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Back Up and Disaster Recovery Policy

All system will be backed up using the following methodologies.

On-site and offsite bare-metal backups for complete image recovery

Offsite file backups.

Security policies and user access control backup.

Document version control.

Disaster recovery is implemented as described in the clients' disaster recovery plan.

Employee Training Policy

PSI will assist client in obtaining Information Security training from an accredited firm. Employee training will occur annually. New employees will complete training prior to being granted access to systems. All training shall conclude with tests that must be completed successfully, be verifiable and recorded.

Penetration Testing Policy

PSI recommends annual internal penetration testing by a third party. PSI will assist and grant access as needed. PSI upon receipt of any report detailing any

security flaw or deficiency will make changes as recommended and documented by testing firm.

Security Monitoring Policy

Client network is to be monitored with an intrusion detection system (IDS) capable of issuing alerts via email and text message. Such system shall be tested during any third-party penetration tests. Client firewall to monitored with a secondary IDS with alerting capabilities. This device will also be tested during any third-party tests.