Secure Configuration Management

Purpose

Secure configurations are used to remove default accounts, passwords, unnecessary services, and other functionality that ship with default configurations in products used by the enterprise. These default configurations may introduce weaknesses that are under the responsibility of the enterprise using the assets. Additionally, secure configurations sometimes enable security-relevant tools and settings that are not available by default. This *Secure Configuration Management* standard provides the processes and procedures for identifying, applying, and maintaining secure configurations throughout the lifetime of all assets and services.

Responsibility

IT is responsible for all secure configurations. This information is relayed to other business units within the enterprise such as finance, accounting, and cybersecurity as required or needed. IT is responsible for informing all users of their responsibilities in the use of any assets assigned to them.

Exceptions

Exceptions to this policy are likely to occur. Requests for exception must be made in writing and must contain:

- The reason for the request,
- Risk to the enterprise of not following the written policy,
- Specific mitigations that will not be implemented,
- Technical and other difficulties, and
- Date of review.

Policy

Plan

1. Configuration guidelines must be selected based on either vendor-provided hardening requirements or industry standards (e.g., Center for Internet Security (CIS) Benchmarks™).
    a. A set of secure configurations must be selected for all operating systems or applications before they are used by the enterprise.
    b. A set of secure configurations must be selected for all cloud platforms or third-party services before they are used by the enterprise.
    c. A set of secure configurations must be selected for all network appliances before they are used by the enterprise.
    d. If configuration guidelines are not available for a particular technology, IT must research appropriate security configurations before using the product to develop a configuration template for this technology.

Implement

1. Every operating system, application, and device deployed in the enterprise network must be appropriately configured and meet security requirements for their individual purposes.
    a. Automatic session expirations must be configured for operating systems and applications where supported, with the period not exceeding 15 minutes.

I. For mobile end-user devices, the automatic session expiration period must not exceed 2 minutes.

b. All enterprise laptops and workstations must utilize a host-based firewall or port-filtering tool, with a default-deny rule.

c. Servers must utilize either a virtual firewall, operating system firewall, or a third-party firewall agent enabled and appropriately configured in accordance with the enterprise's standards.

d. Default accounts shipped with operating systems and software, such as root, administrator, and other pre-configured vendor accounts must be appropriately disabled or configured to prevent unauthorized access (e.g., unauthorized password change).

e. Operating systems must be configured to automatically update, unless an alternative approved patching process is used.

f. Applications must be configured to automatically update, unless an alternative approved patching process is used.

g. All software authorized for use within the enterprise must be currently supported by the developer.

I. Browsers used on all user systems must be currently supported by the developer.

II. Email clients used on all user systems must be fully supported by the developer.

h. IT must configure access control lists on enterprise assets in accordance with the user's need to know. This is to include laptops, smartphones, tablets, centralized file systems, remote file systems, databases, and all applications.

i. IT must ensure that detailed audit logging is enabled for user devices.

j. IT must ensure that sufficient space is available on enterprise assets to collect and maintain audit logs.

k. All instances of the Windows Operating System must disable autorun and autoplay functionality from executing on removable media.

2. Every cloud platform deployed must be appropriately configured in accordance with enterprise standards and meet security requirements for their individual purpose.

   a. IT must configure cloud platforms to enable detailed audit logging.

3. Every network appliance deployed in the enterprise must be appropriately configured and meet security requirements for their individual purpose.

   a. Automatic session expirations must be configured for network appliances.

   b. Default accounts shipped with network appliances, such as root, administrator, and other pre-configured vendor accounts must be appropriately disabled or configured to prevent inappropriate access (e.g., password change).

   c. All ports, protocols, and services not required to support operations must be disabled where possible.

   d. Domain Name System (DNS) filtering services must be used on all enterprise assets to block access to known malicious domains.

   e. IT must configure network appliances to have detailed audit logging enabled.

   f. IT must ensure that sufficient space is available to collect and maintain audit logs.

   g. All network devices and other infrastructure must be configured to automatically update, unless an alternative approved patching process is used.

   h. IT must only use up-to-date network management protocols (e.g., Secure Shell (SSH)

Monitor

1. Securely configured technologies must be monitored to ensure they remain in compliance with approved configurations.

Modify

1. The approved secure configuration guidance for a technology must be updated in a timely manner when a significant update occurs. Significance should be defined by enterprise standards and thresholds.
2. All protocols and tools used to install, modify, or otherwise manage technology configurations must be approved by IT.

Revision History

Each time this document is updated, this table should be updated
.

Version	Revision Date	Revision Description	Name
v1.0	01/22/2023	Initial Written Standard	Scott Tisinger