Secure Configuration Management Policy Template

**CIS Critical Security Controls**

**November 2022**

# Contents

[Contents 2](#_Toc117259947)

[Acknowledgments 3](#_Toc117259948)

[Introduction 4](#_Toc117259949)

[Purpose 4](#_Toc117259950)

[Configurable Devices 4](#_Toc117259951)

[Scope 5](#_Toc117259952)

[Configuration Process 6](#_Toc117259953)

[Further Discussion and Resources 7](#_Toc117259954)

[Secure Configuration Management Policy Template 8](#_Toc117259955)

[Purpose 8](#_Toc117259956)

[Responsibility 8](#_Toc117259957)

[Policy 8](#_Toc117259958)

[Revision History 10](#_Toc117259959)

[Appendix A: Acronyms and Abbreviations 11](#_Toc117259960)

[Appendix B: Glossary 12](#_Toc117259961)

[Appendix C: Implementation Groups 14](#_Toc117259962)

[Appendix D: CIS Safeguards Mapping 15](#_Toc117259963)

[Appendix E: References and Resources 18](#_Toc117259964)

# Acknowledgments

The Center for Internet Security® (CIS®) would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls® (CIS Controls®) and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

**Editors:**

Joshua M Franklin, CIS
Ginger Anderson, CIS

**Contributors:**

Dave Tchozewski
Tony Krzyzewski, SAM for Compliance Ltd
Jon Matthies
Edsel Medina
Staffan Huslid, Truesec
Jamie Fike
Ken Muir
Luke McFadden
Diego Bolatti, Information Systems Engineer, Universidad Tecnológica Nacional (Argentina)
Bryan Chou, CISSP, GSEC, GCED, GCIH
Bryan Ferguson
Keala Asato
Gavin Willbond, SSS – IT Security Specialists
Robin Regnier, CIS
Valecia Stocchetti, CIS

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License. (The link can be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>.)

To further clarify the Creative Commons license related to the CIS Controls® content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization, and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to <http://www.cisecurity.org/controls/> when referring to the CIS Controls in order to ensure that users are employing the most up-to-date guidance. Commercial use of the CIS Controls is subject to the prior approval of the Center for Internet Security, Inc. (CIS®).

# Introduction

As delivered from developers, manufacturers, and resellers, the default configurations for enterprise assets and software are normally geared towards ease-of-deployment and ease-of-use rather than security. Permissive settings, open services and ports, default accounts or passwords, older (vulnerable) protocols, and pre-installation of unnecessary software can all be exploitable if left in their default state. Further, these security configuration updates need to be managed and maintained over the lifetime of all enterprise assets and software. Configuration updates need to be tracked and approved through a configuration management workflow process to maintain a record that can be reviewed for compliance, leveraged for incident response, and to support audits. Secure configurations are important to on-premises devices, as well as remote devices, network devices, and cloud environments.

## Purpose

The CIS Critical Security Controls® (CIS Controls®) include multiple policies that an enterprise should have in place. This policy applies to *CIS Control 4 – Secure Configuration of Enterprise Assets and Software*. Safeguards 4.1 and 4.2 state:

**4.1 - Establish and Maintain a Secure Configuration Process**

Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/IoT devices; and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

**4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure**

Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

This policy is meant as a “jumping off point” for enterprises needing to draft their own secure configuration management policies. Enterprises are encouraged to use this policy template in whole or in part. With that said, there are multiple decisions points and areas that must be tailored to your enterprise; some of which are explored by this document.

## Configurable Devices

Enterprise assets are often not set up by default in the most secure configuration. This is often done to provide flexibility for their customers to apply their own secure configurations in accordance with their own security policies, but also to ensure the product functions “out of the box”. Therefore, the presence of default accounts or passwords, excessive access, or unnecessary services are common in default configurations. These could introduce weaknesses that are under the responsibility of the enterprise using the asset. Even after a strong initial configuration is developed and applied, it must be continually managed to avoid degrading security as software is updated or patched, new security vulnerabilities are reported, and configurations are “tweaked,” to allow the installation of new software or to support new operational requirements.

There are a variety of enterprise, software, and other assets and services that may require configuration. These include hardware, software, and third-party services. Common examples include:

* Operating system configuration: This includes modifying the settings for the common operating systems such as Microsoft® Windows, Apple® MacOS, and the various flavors of Linux® and Unix. Smartphones, tablets, wearables, and internet of things (IoT) devices may all be configurable to various extents.
* Applications: Software written for any platform may require configuration. This includes software written for laptops, servers, smartphones, tablets, wearables, and IoT devices. Databases, hypervisors, and, virtual machines may also be included.
* Cloud services and platforms: Third-party service providers may provide entire platforms that can be configured. These platforms may also provide individual applications that may be configured.
* Network appliances: These all-in-one physical boxes aids in the flow to network connected devices. These include routers, switches, firewalls, wireless access points (WAPs).

## Scope

This policy template is meant to supplement the CIS Controls v8. The policy statements included within this document can be used by all CIS Implementation Groups (IGs) but are specifically geared towards Safeguards in Implementation Group 1 (IG1). In [Appendix D](#_Appendix_D:_CIS), Safeguards unique to IG1 are specifically highlighted for ease of use. For more information on the CIS Implementation Groups, see [Appendix C](#_Appendix_C:_Implementation). Additionally, a glossary in [Appendix B](#_Appendix_B:_Definitions) is provided for guidance on terminology used throughout the document. Future versions of this template may expand the scope to both Implementation Group 2 (IG2) Safeguards. IG2 and IG3 enterprises may feel the need to add sections that go beyond IG1 and are welcome to do so. Depending on an enterprise’s sector or mission, other policy statements may also need to be added or removed. This is encouraged as this policy needs to be molded and fit to the enterprise’s needs.

# Secure Configuration Management Process

There are many ways to create a secure configuration process. This policy divides the process into four smaller elements to help enterprises develop a process that works for them. The process used by this Policy Template is as follows:



Figure 1. Secure Configuration Management Process Diagram

* **Plan** – Creating a process to identify secure configuration baselines, implement them, and then monitor their performance. This may also include creating secure configurations for specific technologies
* **Implement** – Using the secure configuration baselines that were selected, by implementing recommended changes to the various technologies within the enterprise. This should include a validation process to ensure the configuration baselines conform to expectations.
* **Monitor** – As systems are updated and change over time, secure configurations need to be updated. These changes need to be reviewed before implementation.
* **Modify** – Ensuring a particular system is in-line with the approved baseline. This may include discovering new assets or detecting unauthorized changes to a system.

**Plan**

Creating and implementing a process for secure configurations can be difficult. Nearly all the devices in an enterprise can be configured to some extent. All the devices within an enterprise asset inventory, alongside all the software applications within the software inventory, will require some level of configuration. Yet not all assets are equal in importance. Configuring certain assets before others may be logical if that asset is storing or processing sensitive information. Deciding what to configure, how to do it, and when to double check configurations, all falls under the planning element of the secure configuration process.

An enterprise needs to identify and approve secure configuration baselines for all technologies it uses. Secure configuration may be provided from the vendor of a product or service or may be provided by a trusted external organization such as CIS. If no guidance is available, enterprises should perform their own research before using a product. This may lead to the enterprise developing their own configuration guidance. Areas to investigate for secure configuration may include:

* Anti-malware capabilities
* Access control, include user accounts and authentication credentials
* Encryption
* Logging
* Least privilege
* Leveraging hardware security capabilities when possible
* Disabling of unused services, applications, and functionality
* Network connections
* Automatic session locking
* Removal default accounts

**Implement**

Once secure configuration baselines are created and/or selected, IT staff need to configure the technologies in accordance with the baselines. This often involves accessing configuration settings and admin panels within operating systems, firewalls, and other systems. Each element in an approved baseline will need to be implemented and must be tracked by IT staff as required by the enterprise. Some baselines require changes that an enterprise cannot support, such as turning off a necessary feature. Analyzing which baseline modifications can and cannot be made is a process known as “tailoring” and is quite normal. IT will need to keep track of their new and modified baseline. Automated tools can be used to simplify this process and ensure each change is put into place methodically and without error.

**Monitor**

Enterprise assets need to be regularly reviewed for deviations from an approved secure configuration. This can be done manually, or with automated tools. Manual monitoring may include an audit of enterprise assets on a regular, predefined schedule. A change configuration process will ensure only appropriate modifications are made to enterprise assets and that these changes do not introduce vulnerabilities or introduce system instability and/or failure into a network. These changes may need to be tested before being put into production within an enterprise, but some enterprises will be unable to test beforehand.

**Modify**

Once the monitoring phase is complete, changes need to be made accordingly. Certain configuration changes may require patches and other software updates that will push the enterprise back to the *Implement* phase. In addition to making changes identified in the monitoring phase, enterprises will need to keep secure configuration baselines up to date. New versions of software and systems will be released on a regular schedule and need to be re-configured. New baselines will need to be analyzed and reapproved.

## Further Discussion and Resources

**Automated Tooling for Secure Configuration**

Commercial and/or free configuration management tools, such as the CIS Configuration Assessment Tool (CIS-CAT®), <https://learn.cisecurity.org/cis-cat-lite>, can be deployed to measure the settings of operating systems and applications of managed machines to look for deviations from the standard image configurations. Commercial configuration management tools use some combination of an agent installed on each managed system, or agentless inspection of systems through remotely logging into each enterprise asset using administrator credentials. Additionally, a hybrid approach is sometimes used whereby a remote session is initiated, a temporary or dynamic agent is deployed on the target system for the scan, and then the agent is removed. Note that this tool is free for US state, local, tribal, and territorial (SLTT) governments to use but is a commercial product.

# Secure Configuration Management Policy Template

## 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 Policy* provides the processes and procedures for identifying, applying, and maintaining secure configurations throughout the lifetime all asset 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](https://www.cisecurity.org/cis-benchmarks/)™).
2. A set of secure configurations must be selected for all operating systems or applications before they are used by the enterprise.
3. A set of secure configurations must be selected for all cloud platform or third-party services before they are used by the enterprise.
4. A set of secure configurations must be selected for all network appliances before they are used by the enterprise.
5. 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.
2. Automatic session expirations must be configured for operating systems and applications where supported, with the period not exceeding 15 minutes.
3. For mobile end-user devices, the automatic session expiration period must not exceed 2 minutes.
4. All enterprise laptops and workstations must utilize a host-based firewall or port-filtering tool, with a default-deny rule.
5. 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.
6. 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).
7. Operating systems must be configured to automatically update, unless an alternative approved patching process is used.
8. Applications must be configured to automatically update, unless an alternative approved patching process is used.
9. All software authorized for use within the enterprise must be currently supported by the developer.
10. Browsers used on all user systems must be currently supported by the developer.
11. Email clients used on all user systems must be fully supported by the developer.
12. IT must configure access control lists on enterprise assets in accordance with user’s need to know. This is to include laptops, smartphones, tablets, centralized file systems, remote file systems, databases, and all applications.
13. IT must ensure that detailed audit logging is enabled for user devices.
14. IT must ensure that sufficient space is available on enterprise assets to collect and maintain audit logs.
15. All instances of the Windows Operating System must disable autorun and autoplay functionality from executing on removable media.
16. Every cloud platform deployed must be appropriately configured in accordance with enterprise standards and meet security requirements for their individual purpose.
17. IT must configure cloud platforms to enable detailed audit logging.
18. Every network appliance deployed in the enterprise must be appropriately configured and meet security requirements for their individual purpose.
19. Automatic session expirations must be configured for network appliances.
20. 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).
21. All ports, protocols, and services not required to support operations must be disabled where possible.
22. Domain Name System (DNS) filtering services must be used on all enterprise assets to block access to known malicious domains.
23. IT must configure network appliances to have detailed audit logging enabled.
24. IT must ensure that sufficient space is available to collect and maintain audit logs.
25. All network devices and other infrastructure must be configured to automatically update, unless an alternative approved patching process is used.
26. 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. Significant 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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Appendix A: Acronyms and Abbreviations

|  |  |
| --- | --- |
| CIS | Center for Internet Security |
| CIS Benchmarks | Center for Internet Security Benchmarks |
| CIS-CAT | Center for Internet Security Configuration Assessment Tool |
| CIS Controls | Center for Internet Security Critical Security Controls |
| COTS | Commercial-off-the-shelf |
| DNS | Domain Name System |
| IaaS | Infrastructure as a Service (IaaS) |
| IG | Implementation Group |
| IoT | Internet of Things |
| IT | Information Technology |
| SLTT | State, Local, Tribal, and Territorial |
| SSH | Secure Shell |
| WAP | Wireless Access Points |

# Appendix B: Glossary

|  |  |
| --- | --- |
| Asset | Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).Source: [Asset(s) - Glossary | CSRC (nist.gov)](https://csrc.nist.gov/glossary/term/asset) |
| Asset inventory  | An asset inventory is a register, repository or comprehensive list of an enterprise’s assets and specific information about those assets.Source: [Asset Inventory | FTA (dot.gov)](https://www.transit.dot.gov/TAM/resources/assetinventory) |
| Asset owner | The department, business unit, or individual responsible for an enterprise asset.Source: CIS |
| Cloud environment | A virtualized environment that provides convenient, on-demand network access to a shared pool of configurable resources such as network, computing, storage, applications, and services. There are five essential characteristics to a cloud environment: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Some services offered through cloud environments include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). |
| Enterprise assets | Assets with the potential to store or process data. For the purpose of this document, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers in virtual, cloud-based, and physical environments.Source: CIS Controls v8  |
| End-user devices | Information technology (IT) assets used among members of an enterprise during work, off-hours, or any other purpose. End-user devices include mobile and portable devices such as laptops, smartphones, and tablets as well as desktops and workstations. For the purpose of this document, end-user devices are a subset of enterprise assets.Source: CIS Controls v8 |
| Enterprise asset identifier  | Often a sticker or tag with a unique number or alphanumeric string that can be tracked within an enterprise asset inventory.Source: CIS |
| Mobile end-user devices | Small, enterprise-issued end-user devices with intrinsic wireless capability, such as smartphones and tablets. Mobile end-user devices are a subset of portable end-user devices, including laptops, which may require external hardware for connectivity. For the purpose of this document, mobile end-user devices are a subset of end-user devices.Source: CIS Controls v8 |
| Network devices | Electronic devices required for communication and interaction between devices on a computer network. Network devices include wireless access points, firewalls, physical/virtual gateways, routers, and switches. These devices consist of physical hardware as well as virtual and cloud-based devices. For the purpose of this document, network devices are a subset of enterprise assets.Source: CIS Controls v8 |
| Non-computing/Internet of Things (IoT) devices | Devices embedded with sensors, software, and other technologies for the purpose of connecting, storing, and exchanging data with other devices and systems over the internet. While these devices are not used for computational processes, they support an enterprise’s ability to conduct business processes. Examples of these devices include printers, smart screens, physical security sensors, industrial control systems, and information technology sensors. For the purpose of this document, non-computing/IoT devices are a subset of enterprise assets.Source: CIS Controls v8 |
| Physical environment | Physical hardware parts that make up a network, including cables and routers. The hardware is required for communication and interaction between devices on a network.Source: CIS Controls v8 |
| Portable end-user devices | Transportable, end-user devices that have the capability to wirelessly connect to a network. For the purpose of this document, portable end-user devices can include laptops and mobile devices such as smartphones and tablets, all of which are a subset of enterprise assets.Source: CIS Controls v8 |
| Remote devices | Any enterprise asset capable of connecting to a network remotely, usually from public internet. This can include enterprise assets such as end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers.Source: CIS Controls v8 |
| Servers | A device or system that provides resources, data, services, or programs to other devices on either a local area network or wide area network. Servers can provide resources and use them from another system at the same time. Examples include web servers, application servers, mail servers, and file servers.Source: CIS Controls v8 |
| User | Employees (both on-site and remote), third-party vendors, contractors, service providers, consultants, or any other user that operates an enterprise asset.Source: CIS |
| Virtual environment | Simulates hardware to allow a software environment to run without the need to use a lot of actual hardware. Virtualized environments are used to make a small number of resources act as many with plenty of processing, memory, storage, and network capacity. Virtualization is a fundamental technology that allows cloud computing to work.Source: CIS Controls v8 |

# Appendix C: Implementation Groups

As a part of our most recent version of the CIS Controls, v8, we created Implementation Groups (IGs) to provide granularity and some explicit structure to the different realities faced by enterprises of varied sizes.

**IG1**

An IG1 enterprise is small- to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

**IG2**

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information, and they can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

**IG3**

An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

If you would like to know more about the Implementation Groups and how they pertain to enterprises of all sizes, there are many resources that explore the Implementation Groups and the CIS Controls in general on our website at <https://www.cisecurity.org/controls/cis-controls-list/>.

# Appendix D: CIS Safeguards Mapping

**CIS Controls & Safeguards Covered by this Policy**

This policy helps to bolster IG1 Safeguards in CIS Control 4: *Secure Configuration of Enterprise Assets and Software*. Table 1 shows which IG1 Safeguards are covered by this policy as written.

Table - Safeguards covered by IG1

|  |  |  |  |
| --- | --- | --- | --- |
| CIS Control | Policy Statement | CIS Safeguard | CIS Safeguard Description |
| 3.3 | Implement 1h, 3b | Configure Data Access Control Lists | Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |
| 4.1 | Plan1, 1a, 1b, 1d | Establish and Maintain a Secure Configuration Process | Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/IoT devices; and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |
| 4.2 | Plan 1cImplement 3c | Establish and Maintain a Secure Configuration Process for Network Infrastructure | Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |
| 4.3 | Implement 1a, 1ai, 3a | Configure Automatic Session Locking on Enterprise Assets | Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |
| 4.4 | Implement 1c | Implement and Manage a Firewall on Servers | Implement and manage a firewall on servers, where supported operating system firewall, or a third-party firewall agent. |
| 4.5 | Implement 1b | Implement and Manage a Firewall on End-User Devices | Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |
| 4.6 | Implement 3h | Securely Manage Enterprise Assets and Software | Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential. |
| 4.7 | Implement 1d | Manage Default Accounts on Enterprise Assets and Software | Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable. |
| 7.3 | Implement 1e | Perform Automated Operating System Patch Management | Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. |
| 7.4 | Implement 1f | Perform Automated Application Patch Management | Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. |
| 8.2 | Implement 1i, 2d, 3e | Collect Audit Logs | Collect audit logs. Ensure that logging, per the enterprise’s audit log management process, has been enabled across enterprise assets. |
| 8.3 | Implement 2a, 3f | Ensure Adequate Audit Log Storage | Ensure that logging destinations maintain adequate storage to comply with the enterprise’s audit log management process. |
| 9.1 | Implement 1gi, 1gii | Ensure Use of Only Fully Supported Browsers and Email Clients | Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor |
| 9.2 | Implement 3d | Use DNS Filtering Services | Use DNS filtering services on all enterprise assets to block access to known malicious domains. |
| 10.3 | Implement k | Disable Autorun and Autoplay for Removable Media | Disable autorun and autoplay auto-execute functionality for removable media. |

|  |  |  |  |
| --- | --- | --- | --- |
| 12.1 | Implement 3g | Ensure Network Infrastructure is Up-to-Date | Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support. |

# Appendix E: References and Resources

Center for Internet Security®

<https://www.cisecurity.org/>

CIS Benchmarks
https://www.cisecurity.org/cis-benchmarks/

CIS Configuration Assessment Tool (CIS-CAT®)
<https://learn.cisecurity.org/cis-cat-lite>

CIS Critical Security Controls®

<https://www.cisecurity.org/controls/>