Software Asset Management Policy Template

**CIS Critical Security Controls**

**November 2022**

# Contents

[Contents 2](#_Toc117259970)

[Acknowledgments 3](#_Toc117259971)

[Introduction 4](#_Toc117259972)

[Purpose 4](#_Toc117259973)

[Types of Software Assets 4](#_Toc117259974)

[Scope 5](#_Toc117259975)

[Software Asset Lifecycle 6](#_Toc117259976)

[Software Asset Management Policy Template 9](#_Toc117259977)

[Purpose 9](#_Toc117259978)

[Responsibility 9](#_Toc117259979)

[Policy 9](#_Toc117259980)

[Revision History 11](#_Toc117259981)

[Appendix A: Acronyms and Abbreviations 12](#_Toc117259982)

[Appendix B: Glossary 13](#_Toc117259983)

[Appendix C: Implementation Groups 15](#_Toc117259984)

[Appendix D: CIS Safeguards Mapping 16](#_Toc117259985)

[Appendix E: References and Resources 17](#_Toc117259986)

# 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

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

Software asset management is the process of procuring, identifying, tracking, maintaining, and removing software on enterprise assets. Software asset management is a difficult problem for an enterprise of any size. New software is constantly acquired within an enterprise. Software must be maintained, updated, and ultimately uninstalled. Additionally, users may attempt to install unauthorized software on enterprise assets. With work from home becoming more prominent, software may be regularly used on enterprise assets that are not actively connected to the enterprise network. This necessitates that software may be managed by an enterprise’s Information Technology (IT) personnel

## Purpose

The Center for Internet Security® (CIS®) recommends several policies that an enterprise should have in place. One of those policies, a *Software Asset Management Policy,* is meant as a “jumping off point” for enterprises that need help drafting their own software asset management policy. 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. As an example, deciding and documenting which “departments” or “business units” are responsible for asset management. In CIS Controls v8, Control 2 states:

**Control 2 – Inventory and Control of Software Assets**

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

To support this Safeguard, it is important for an enterprise to develop a software asset management process. This process should include establishing and maintaining a detailed software asset inventory, ensuring that software is currently supported (e.g., not end-of-life or end-of-support), and addressing unauthorized software, at a minimum. This document supports the development of a process for managing software assets and the implementation of this CIS Control.

## Types of Software Assets

There are many types of software assets that can exist on enterprise assets. For the purposes of this document and as defined in the CIS Critical Security Controls® (CIS Controls®), a software asset (or software, for short) are the programs and other operating information used within an enterprise asset[[1]](#footnote-1).

Software assets include both operating systems and applications. An **operating system** is system software on enterprise assets that manages computer hardware and software resources, and provides common services for programs. Operating systems are considered a software asset and can be single- and multi-tasking, single- and multi-user, distributed, templated, embedded, real-time, and library. An **application** is a program, or group of programs, hosted on enterprise assets and designed for end users. Applications are considered a software asset in this document. Examples include web, database, cloud-based, and mobile applications.

Additionally, there are multiple components that make up applications and operating systems, including services and libraries. A **service** refers to a software functionality or a set of software functionalities, such as the retrieval of specified information or the execution of a set of operations. Services provide a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and based on the identity of the requestor per the enterprise’s usage policies. A **library** is pre-written code, classes, procedures, scripts, configuration data, and more, used to develop software programs and applications. It is designed to assist both the programmer and the programming language compiler in building and executing software



Figure 1. Software assets, as defined in CIS Controls v8

There are also several different types of software. The definitions revolve around the software owner, cost, and the ability to modify and redistribute the code. The following provides general definitions for different software types:

* Free software: Completely free to download, modify, distribute, and use software.
* Freeware: No-cost software that often includes a limited license to specific groups of users (e.g., students). Modification of source code is generally prohibited.
* Open source: Free software for download and use, but the license will dictate stipulations for modification and redistribution.
* Commercial off the Shelf (COTS) software: Software that is publicly available for purchase. Patrons are generally not authorized to modify the software.
* Internally developed applications: Software applications created and maintained by an enterprise and their contractors. The enterprise generally owns all rights save for any licenses used in development stipulating otherwise.
* Shareware: Often a type of software offered with a time-limited license, and potentially limited feature sets. Full versions are made available for purchase.
* Scripts (e.g., PowerShell, Bash): A program that provides a series of instructions to the operating system, typically to accomplish a series of more basic tasks.

## 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.

# Software Asset Management Lifecycle

Shown below in Figure 2 are the high-level “steps” of the *Software Asset Lifecycle,* followed by a detailed description of what each step entails. Identifying and tracking software assets is an important process in the *Software Asset Management Lifecycle.* In order to protect a network and its assets, an enterprise must first know what software is on a network. In addition, many other security controls are dependent on the software asset inventory, such as secure configurations, account management, access control, and more.

Figure 2. Software Asset Management Lifecycle

* **Procurement** – Acquiring new software from software vendors and managing software licenses.
* **Installation** – Deploying new software products to employee assets, to include phones, tablets, desktops, servers, and cloud infrastructure.
* **Discovery** – The identification of software by actively searching systems connected to the enterprise network.
* **Usage** – The authorized use of approved software by employees.
* **Update and Upgrade** – Applying minor software patches or replacing a software asset with new functionality.
* **Removal** – Deleting or retiring software from enterprise assets.

**Procurement**

The procurement process generally consists of purchasing new software from external vendors, including from managed service providers (MSPs) and cloud service providers (CSPs), or obtaining new software by transfer from another business unit within the same enterprise. Those individuals charged with making purchasing decisions, often from the IT or financial business units, should evaluate all vendors before making a purchase. There should be a pre-defined process in place to ensure the vendor is reputable and that major components are not left out of any contracts.

CIS provides a [simple template](https://www.cisecurity.org/insights/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet) for starting an software asset inventory, but many enterprises will quickly find the need to move to something more robust, such as a third-party tool or database. Note that the software asset inventory is likely to contain sensitive information that could be leveraged by malicious parties. Therefore, the inventory should have sufficient access control to prevent unauthorized access and modification.

**Installation**

The installation process generally consists of deploying new services or additional software required for business functions to employee assets, including laptops, desktops, phones, tablets, servers, and cloud infrastructure. This process varies for each software and the device on which it is installed. However, in general it requires code to be copied to local folders on the asset to facilitate access by the operating system. Installation includes the creation of necessary directories and registering environment variables. During this process, IT would ensure the software is configured appropriately, not only for execution but also security purposes.

**Discovery**

Once software applications are installed on enterprise assets, the maintenance process begins. Part of this maintenance process consists of searching for new software on your enterprise assets through the use of freely or commercially available discovery tools. Any new software identified should be added to the software asset inventory.

Once the inventory is updated, either via discovery or other means, it is time to check all discovered software against the known list of approved software. This may take some time, but it is critical from a cybersecurity perspective. Any unauthorized software must be investigated to understand if this is new software that needs to be added to the approved inventory listing or if the software is unauthorized and needs to be removed. Some software may be malicious in nature and must be removed. If a software is deemed to be malicious, it may be pertinent to activate the enterprise’s incident response process.

**Usage**

This phase is the step with the least amount of interaction with IT and cybersecurity, as users are simply using the software they were provisioned with to accomplish their everyday work tasks. A set of rules governing how a user can leverage software to perform their job should be in place and properly communicated to the user. Accordingly, the usage phase of this document contains a sample set of policy statements. It is commonplace for these rules to be placed within a separate policy document called an *Acceptable Use Policy*. The owner of this *Software Asset Management Policy* may choose to delete all content in the usage section and refer to an external *Acceptable Use Policy* that may already be in place. Note that the statements contained within the *Usage* phase of this document are insufficient to act as a fully realized *Acceptable Use Policy*.

**Update & Upgrade**

The upgradeprocess for software entails replacing the software asset with a newer version provided by the developer. Newer versions of software are usually accompanied by major changes or security enhancements, and often drastically change the application, operating system, or software. The update process is the act of modifying already installed software, which consists of patches and *ad hoc* updates that do not consist of major changes to the software. Some enterprises may wish to test updates before they are integrated into production environments. Updates are part of a regular operational process whereas upgrades occur when the enterprise requires additional features or otherwise retire the existing version. This means that software updates occur more frequently than software upgrades, and upgrades may never occur depending on budget or the developer. For additional information please refer to the *Vulnerability Management Policy Template.*

**Removal**

Software removal refers to the process of uninstalling software from an enterprise asset or enterprise environment. Removal may be necessary due to various reasons such as the software is now deemed unauthorized or is no longer necessary for the enterprise’s business functions or mission. Additionally, contracts with vendors may have ended, or software may simply have been superseded by another application. It’s often common to remove software and data from assets when sending a device back for warranty or repair. Removal can be completed manually or with the assistance of tooling. It is important to remember that components of the software may be located in different directories and folders.

**License Management**

All software has a license associated with it. This may be a commercial, open source or an implicit free license. A software license states what can and cannot be done with the software, under what conditions it can be used or modified, for how long, any bounds surrounding distributing the software to others, and potentially more. Abiding to each license is best practice and often the law. Tracking user licenses, maintaining registration fees, complying with licensing terms, and most importantly, determining relevance for each license is a necessity. Most enterprises have a wide range of software and licenses in use every day. A license management system allows enterprises to have a clear view and understanding of the licenses and entitlements that they own, and how they are being used within their environment.

# Software Asset Management Policy Template

## Purpose

Software asset management is the process of procuring, identifying, tracking, maintaining, and removing software on enterprise assets. This *Software Asset Management Policy* provides the policies for governing the software asset lifecycle while an enterprise is using a software asset. A software inventory must be created and maintained to support the enterprise’s mission and to help ensure only authorized software is installed and used. This software inventory must be up-to-date and reflect the current state of software across the enterprise.

## Responsibility

The IT business unit is responsible for all software asset management functions. This information is relayed to other business units within the enterprise such as finance, accounting, and cybersecurity as 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

**Procurement**

1. Only individuals from IT are approved to procure software.
2. IT must maintain a list of approved software vendors.
3. Software must only be purchased from vendors on the approved software list.

**Installation**

1. Any software installed on enterprise assets, alongside other relevant information within the software asset, must be recorded within the software inventory. This must include:
2. Title of software
3. Developer or publisher of software
4. Date of acquisition
5. Date of installation
6. Duration of usage
7. Business purpose
8. App Store(s)
9. Version(s)
10. Uniform Resource Locator (URL)
11. Deployment mechanism
12. End-of-support (EoS) date, if known
13. End-of-life (EoL) date, if known
14. Any relevant licensing information
15. Decommission date
16. IT must verify the software asset inventory every six months, or more frequently as needed.
17. Only software that has been approved by IT may be installed.
18. Only cloud services that have been approved by IT may be used within the enterprise.
19. Mobile devices may only obtain software from IT approved sources.

**Usage**

**In general, refer to the enterprise’s *Acceptable Use Policy*.**

There are no IG1 safeguards that support this portion of the software asset management process.

**Discovery**

1. IT must review all software installed on enterprise assets on a monthly basis.
2. All installed software on enterprise assets must be reported to IT on a regular basis.
3. All newly discovered software must be checked against the list of approved software in the software asset inventory.
4. Identified software not included within this inventory must be investigated as the software may be unauthorized.
5. Assets containing unauthorized software must be removed from the network unless temporary access is granted by the IT business unit.
6. The presence of unauthorized software must be properly investigated.
7. All newly discovered (authorized) software must be added to the software inventory.
8. Unauthorized software must be removed from use on enterprise assets or receive a documented exception.

**Update and Upgrade**

1. All updates and upgrades must be approved by IT prior to installation. IT configuring a device for automatic updates, or directing users to do so, constitutes a tacit approval.

**Removal**

1. Software to be decommissioned must be removed from all enterprise assets.
2. Assets containing retired software must be protected with additional defensive mitigations, such as removal from the network or isolation.
3. IT must make a copy of the user data as needed.
4. Ensure that any retired software did not store data in other servers or cloud infrastructure not owned by the enterprise.

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 Controls | Center for Internet Security Critical Security Controls |
| COTS | Commercial-off-the-shelf |
| CSPs | Cloud Service Providers |
| EoL | End of Life |
| EoS | End of Support |
| IG | Implementation Group |
| IoT | Internet of Things |
| IT | Information Technology |
| MSPs | Managed service provider |
| URL | Uniform Resource Locator |

# 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 and Safeguards Covered by this Policy**

This policy helps to bolster IG1 Safeguards in CIS Control 2*: Inventory and Control of Software Assets*. Table 1 shows which IG1 Safeguards are covered by this policy as written.

Table 1 - Safeguards covered by IG1

|  |  |  |  |
| --- | --- | --- | --- |
| CIS Control | Policy Statement | CIS Safeguard  | CIS Safeguard Description |
| 2.1 | Installation 1, 2, 3Discovery 2c | Establish and Maintain a Software Inventory | Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently. |
| 2.2 | Procurement 1, 2, 3Installation 3, 4, 5Update & Upgrade1 | Ensure Authorized Software is Currently Supported | Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise’s mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently. |
| 2.3 | Discovery 1, 1a, 1b, 2, 2a, 2bRemoval 1, 2, 3  | Address Unauthorized Software | Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently. |

# Appendix E: References and Resources

Center for Internet Security®

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

CIS Critical Security Controls®

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

CIS Controls v8 Guide to Enterprise Assets and Software

<https://www.cisecurity.org/insights/white-papers/guide-to-enterprise-assets-and-software>

CIS Controls Hardware and Software Asset Tracking Spreadsheet – (simple template) https://www.cisecurity.org/insights/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet

1. Enterprise assets are defined as all end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers that exist in virtual, cloud-based, or physical environments, including those that can be connected to remotely. Enterprise assets are assets managed by the enterprise and have the potential to store, process, or transmit data. [↑](#footnote-ref-1)