Enterprise Asset Management Policy Template

**CIS Critical Security Controls**

**June 2022**

# Contents

[Contents 2](#_Toc106357962)

[Acknowledgments 3](#_Toc106357963)

[Introduction 4](#_Toc106357964)

[Purpose 4](#_Toc106357965)

[Types of Enterprise Assets 4](#_Toc106357966)

[Scope 5](#_Toc106357967)

[Enterprise Asset Lifecycle 6](#_Toc106357968)

[How To Use This Document 8](#_Toc106357969)

[Applicability to Implementation Groups 8](#_Toc106357970)

[Information Technology and Cybersecurity Business Units 8](#_Toc106357971)

[Enterprise Asset Management Policy Template 9](#_Toc106357972)

[Purpose 9](#_Toc106357973)

[Responsibility 9](#_Toc106357974)

[Policy 9](#_Toc106357975)

[Acquisition 9](#_Toc106357976)

[Discovery 10](#_Toc106357977)

[Usage 10](#_Toc106357978)

[Controlled Disposal 10](#_Toc106357979)

[Uncontrolled Disposal 10](#_Toc106357980)

[Revision History 12](#_Toc106357981)

[Appendix A: Acronyms and Abbreviations 13](#_Toc106357982)

[Appendix B: Glossary 14](#_Toc106357983)

[Appendix C: Implementation Groups 16](#_Toc106357984)

[Appendix D: CIS Safeguards Mapping 17](#_Toc106357985)

[Appendix E: References and Resources 18](#_Toc106357986)

# 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

**Contributors:**

Dave Tchozewski   
Tony Krzyzewski, SAM for Compliance Ltd  
Jon Matthies   
Edsel Medina   
Staffan Huslid, Truesec  
Jaime Fike  
Ken Muir   
Luke McFadden   
Diego Bolatti, Information Systems Engineer, Universidad Tecnológica Nacional (Argentina)   
Bryan Chou, CISSP, GSEC, GCED, GCIH  
Bryan Ferguson  
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

Enterprise asset management is the process of procuring, identifying, tracking, maintaining, and disposing of an asset owned by an enterprise. Enterprise asset management is a difficult problem for an enterprise of any size. New assets are constantly acquired, others are retired, whereas many assets are simply lost. With work from home becoming more prominent, enterprise assets may disappear from the main enterprise network, only to reappear months later, or never again. There are multiple types of enterprise assets that often need to be managed differently. Enterprises may perform asset management in a manual fashion, may employ a database or spreadsheet, or may use dedicated asset management software.

## Purpose

The Center for Internet Security® (CIS®) recommends several policies that an enterprise should have in place. The first of many policies, *Enterprise Asset Management Policy,* is meant as a “jumping off point” for enterprises that need help drafting their own enterprise 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 1 states:

**Control 1 – Inventory and Control of Enterprise Assets –** Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

To support this Safeguard, it is important for an enterprise to develop an enterprise asset management process. This process should include establishing and maintaining a detailed enterprise asset inventory and addressing unauthorized assets, at a minimum. This document supports the development of a process for managing enterprise assets and the implementation of Safeguards in this CIS Control.

## Types of Enterprise Assets

There are many types of enterprise assets that can exist in an enterprise. For the purposes of this document and as defined in CIS Critical Security Controls® v8 (CIS Controls® v8), 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. Types of enterprise assets include:

* *End-user devices*, such as desktops, workstations, laptops, tablets, and smartphones
* *Network devices*, such as wireless access points, switches, firewalls, physical/virtual gateways, and routers
* *Non-computing/Internet of Things (IoT) devices*, such as Industrial Control Systems (ICS), smart screens, printers, physical security sensors, and IT security sensors
* *Servers*, such as web servers, email servers, application servers, and file servers

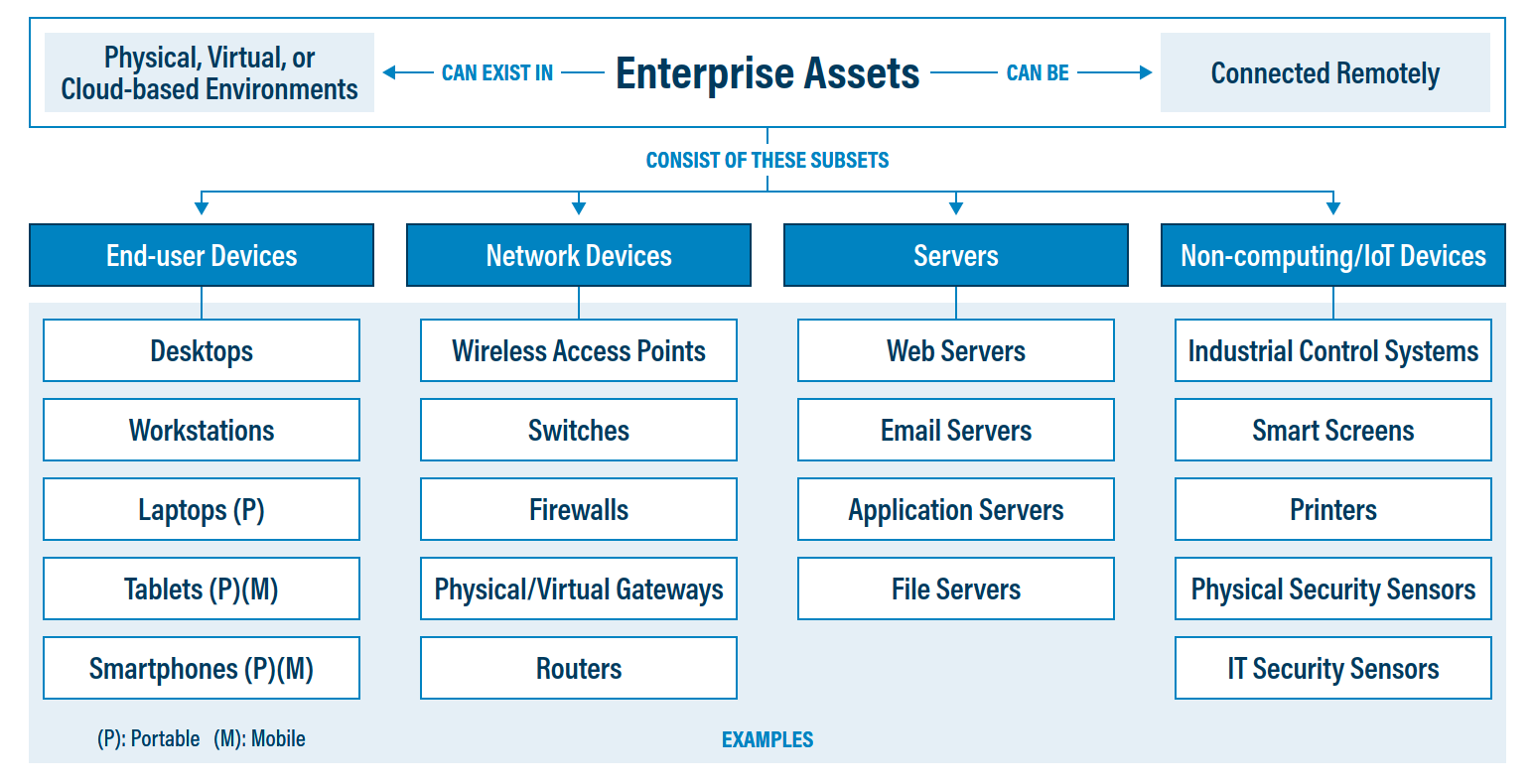


Figure 1. Enterprise assets, as defined in CIS Controls v8

## Scope

This *Enterprise Asset Management Policy* is divided into multiple sections based on usage patterns of assets within an enterprise. Users of this policy template are free to further divide this process into any form that works for your enterprise.

It is important to note that asset management as a whole generally includes [assets](#_Appendix_B:_Glossary) that do not store, process, or transmit data, such as monitors and keyboards. While these assets are important to track and monitor in an enterprise, they are beyond the scope of this document. For the purposes of this document, we will follow the CIS Controls v8 definition of an [enterprise asset](https://www.cisecurity.org/insights/white-papers/guide-to-enterprise-assets-and-software).

# Enterprise Asset Lifecycle

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

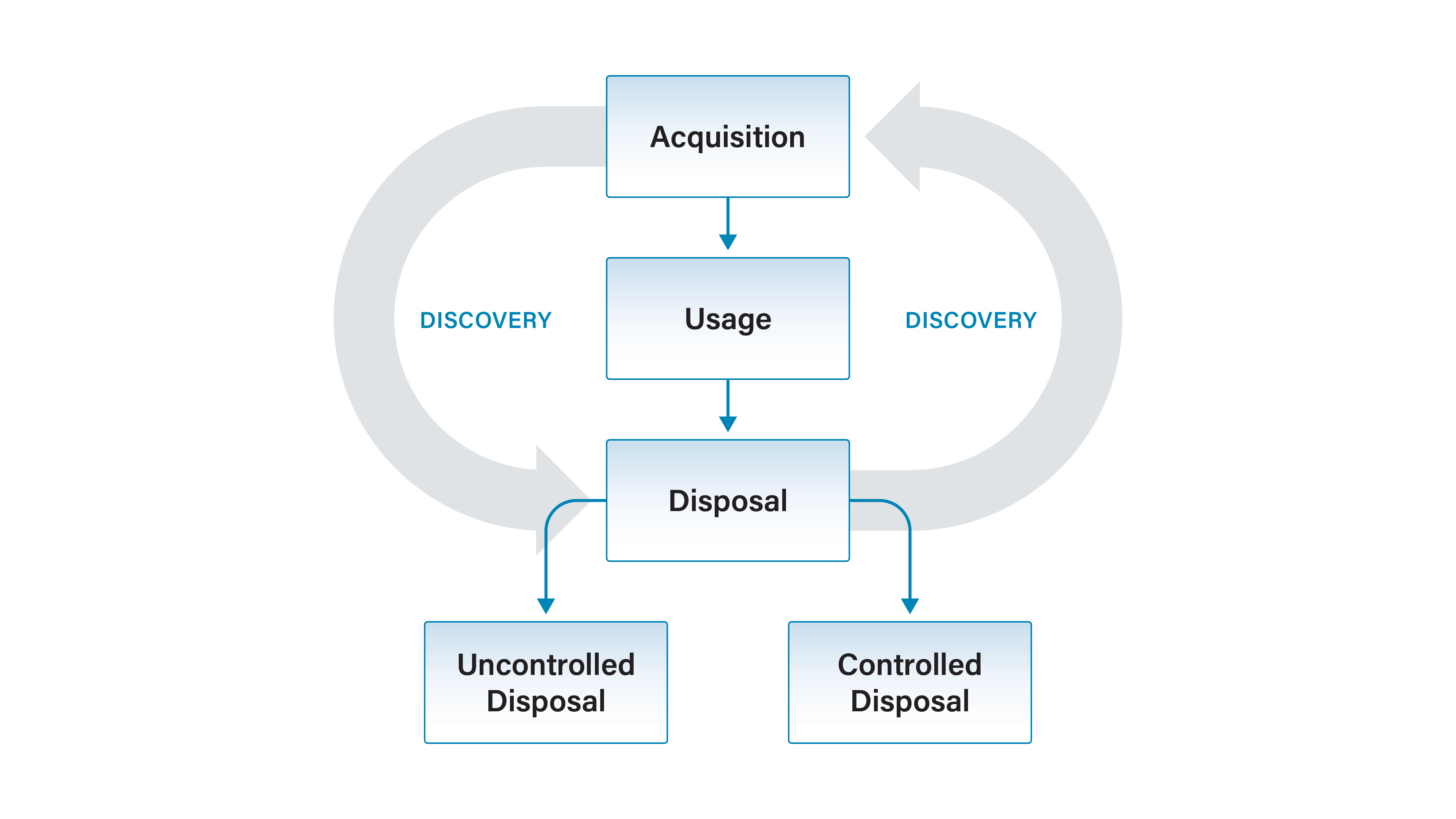


Figure 2. Enterprise Asset Lifecycle

* **Acquisition** – Purchasing new enterprise assets or obtaining new enterprise assets by transfer from another business unit.
* **Discovery** – The identification of new enterprise assets by actively searching for systems connected to the enterprise network. This process is constantly occurring throughout the lifecycle of an enterprise asset.
* **Usage** – The authorized use of enterprise assets by users. For the purposes of this document, users may include employees (both on-site and remote), third-party vendors, contractors, service providers, consultants, or any other user that operates an enterprise asset.
* **Controlled Disposal** – Retiring enterprise assets in a secure manner.
* **Uncontrolled Disposal** – Lost, stolen, or otherwise unaccounted for enterprise assets. As an enterprise grows, this tends to become a regularly occurring issue, and it is worthwhile to discuss the procedures around this before it becomes a problem.

**Acquisition**

The acquisition process generally consists of purchasing new enterprise assets from external vendors, including from managed service providers (MSPs) and cloud service providers (CSPs), or obtaining new enterprise assets 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 enterprise 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 enterprise 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.

**Discovery**

Once an inventory is created, the maintenance process begins. Part of this maintenance process consists of searching for new enterprise assets on your network. Enterprises can use large-scale, comprehensive enterprise products to maintain enterprise asset inventories. Smaller enterprises can leverage security tools already installed on enterprise assets or used on the network to collect this data. To the extent practical, users will need to routinely connect their enterprise assets to the enterprise network to ensure that IT knows which assets are out there and being used. This can be challenging in a world of remote users and regular travel.

Once inventory is taken, either via a scan or other means, it is time to check all discovered enterprise assets against the known list of approved assets. This may take some time, but it is critical from a cybersecurity perspective. Any unauthorized assets that were identified must be investigated to understand if they are new assets that need to be added to the approved inventory listing or if they are assets that need to be removed. These assets may have connected accidentally or may be malicious in nature and must be removed. If an asset is deemed to be malicious, it may be pertinent to activate the enterprise’s incident response process.

**Usage**

The *Usage* phase is the step with the least amount of interaction with IT and cybersecurity, as users are simply operating the enterprise asset they were provisioned with to accomplish their everyday work tasks. A set of rules governing how a user can leverage enterprise assets to perform their job should be in place and properly communicated to the user. Accordingly, the *Usage* phase of this *Enterprise Asset Management Policy* contains a sample set of policy statements. Yet it is commonplace for these rules to be placed within a separate policy document called an *Acceptable Use Policy*. The owner of this *Enterprise Asset Management Policy* may choose to delete all content in the *Usage* section and simply 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*.

**Uncontrolled Disposal**

Users will lose or relinquish their enterprise assets from time to time. Uncontrolled disposal of enterprise assets includes a user losing their device or having it stolen. It is often difficult to tell exactly what occurred. In either scenario, enterprise access from that asset needs to be removed as soon as possible, and the data may need to be wiped from the asset. Users need to be trained to report this occurrence right away so that IT can act quickly. A report should be filed with law enforcement, which is also often required for insurance and liability reasons. The enterprise asset should be noted as stolen or lost in the asset inventory.

**Controlled Disposal**

This phase of the lifecycle will be how enterprise assets reach their end of life. Assets to be decommissioned need to be returned from users to IT so that user data can be retrieved and/or transferred as necessary. Then all enterprise data can be removed from the enterprise asset in a secure fashion as required in the *Data Management Plan*. Enterprise assets may then be sold to third-party providers for resale or securely destroyed. The device should be noted as retired or decommissioned in the enterprise asset inventory. Access to enterprise data should be revoked for this device.

# How To Use This Document

## Applicability to Implementation Groups

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 they 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 will expand the scope to both Implementation Group 2 (IG2) and Implementation Group 3 (IG3) Safeguards. IG2 and IG3 enterprises may feel the need to add sections that go beyond IG1, and they 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.

## Information Technology and Cybersecurity Business Units

The IT department and Cybersecurity department may be separate or distinct business units. Modify this policy template accordingly to reflect which business unit has various responsibilities outlined within the text of the policy. Other business units such as finance and accounting may also play a role within the enterprise asset management process; this should be reflected within this document.

# Enterprise Asset Management Policy Template

## Purpose

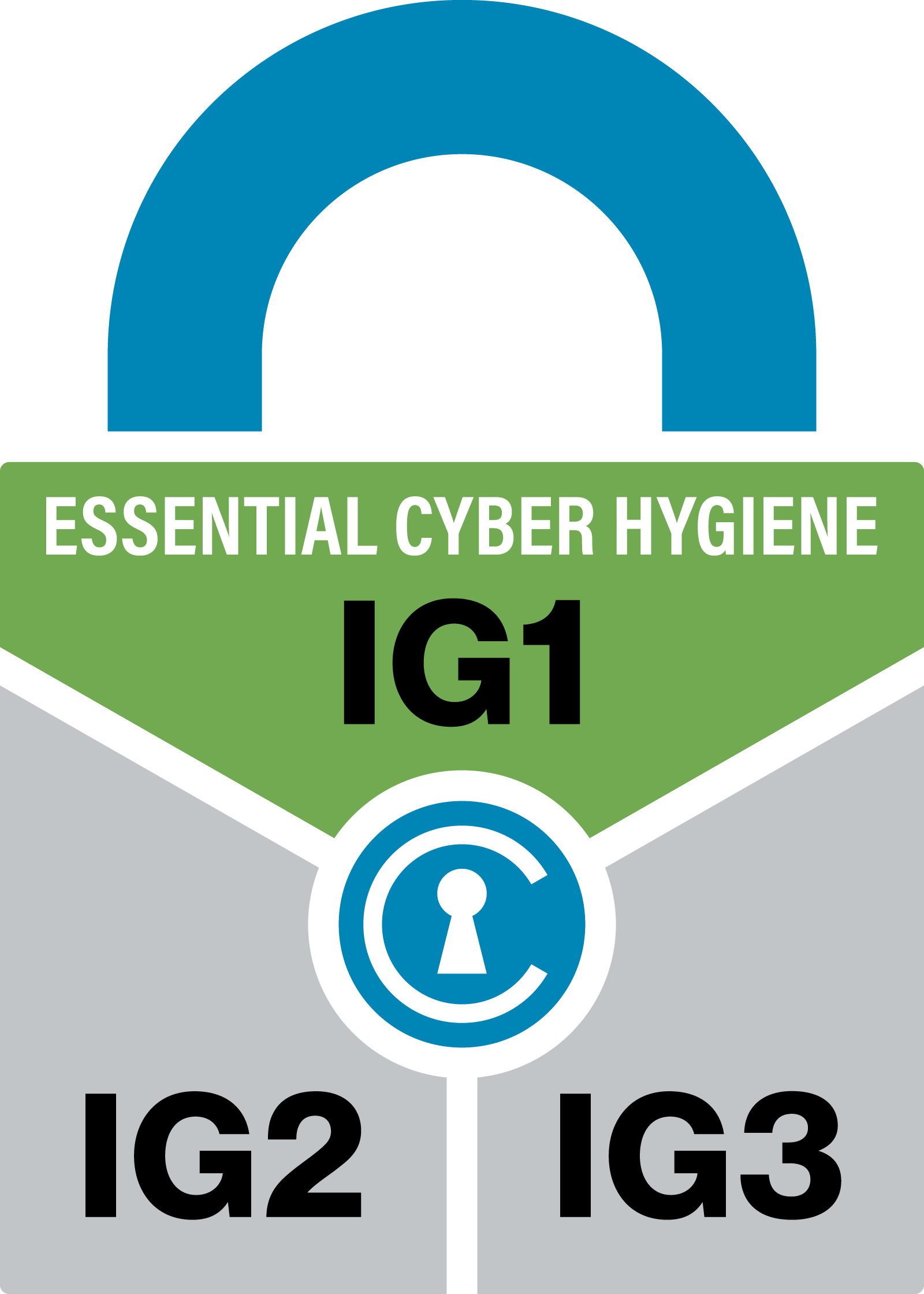
Enterprise asset management is the process of procuring, identifying, tracking, maintaining, and disposing of an asset owned by an enterprise. The *Enterprise Asset Management Policy* provides the processes and procedures for governing the enterprise asset lifecycle while an enterprise is using an asset. An inventory must be created and maintained to support the enterprise’s mission. This inventory must be current and reflect the current assets owned and operated by the enterprise.

## Responsibility

The IT business unit is responsible for all enterprise asset management functions. 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 enterprise assets assigned to them.

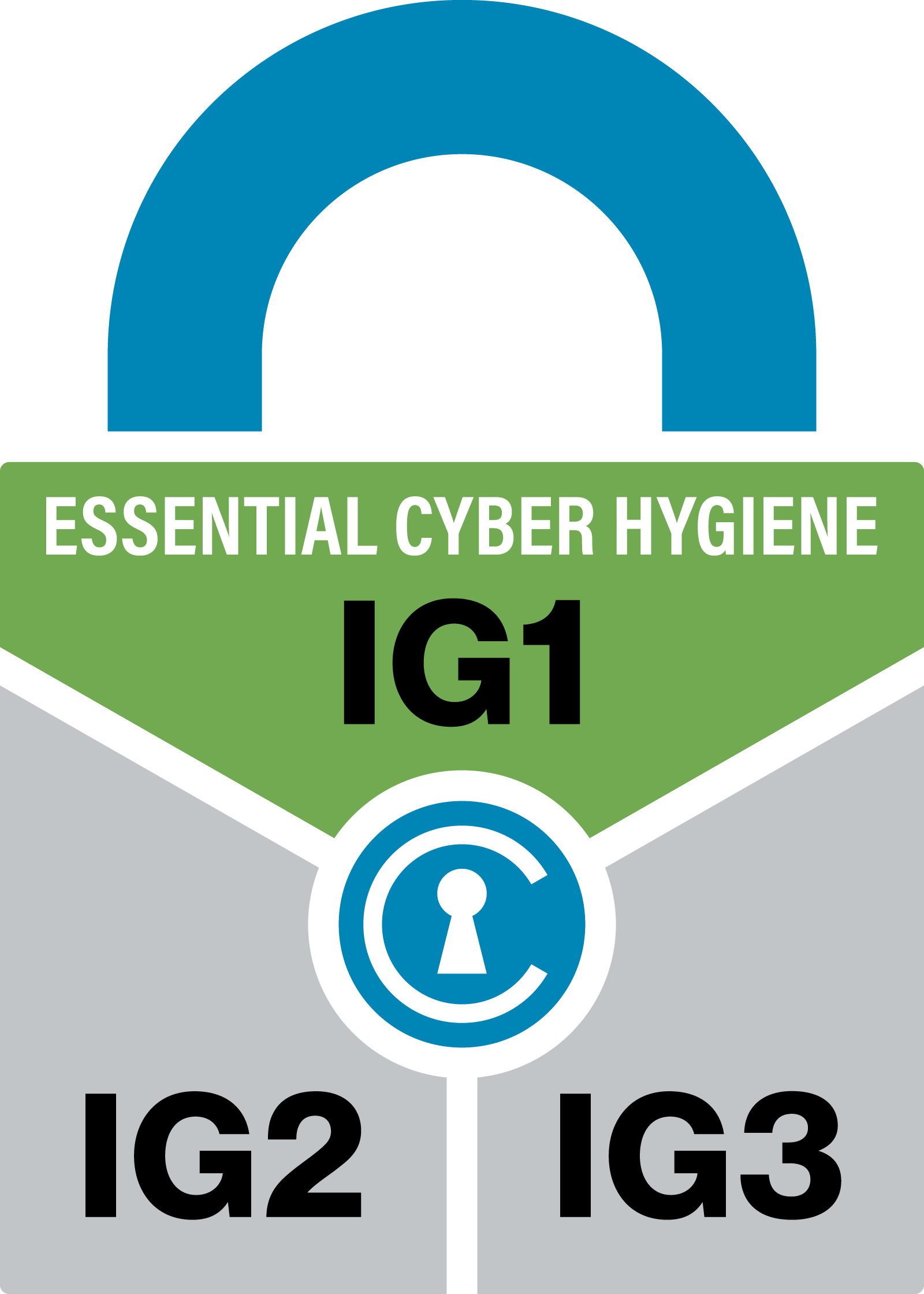
## Policy

### Acquisition

** Implementation Group 1: Safeguard 1.1**

1. The IT business unit shall assign unique identifiers to all existing and newly acquired enterprise assets.
2. Each enterprise asset (e.g., desktops, laptops, servers, tablets), where applicable, must have an enterprise asset tag affixed to the device with this identifier.
3. Record the enterprise asset identifier alongside other relevant information within the IT inventory. This is to include:
   1. Enterprise asset identifier
   2. Date of purchase
   3. Purchase price
   4. Item description
   5. Manufacturer
   6. Model number
   7. Serial number
   8. Name of the enterprise asset owner (e.g., administrator, user), role, or business unit, where applicable.
   9. Physical location of enterprise asset, where applicable
   10. Physical (Media Access Control (MAC)) address
   11. Internet Protocol (IP) address
   12. Warranty expiration date
   13. Any relevant licensing information
4. IT must verify the enterprise asset inventory every six months or more frequently.

### Discovery

** Implementation Group 1: Safeguard 1.2**

1. Enterprise assets not included within the inventory must be investigated, as these assets may be unauthorized.
   1. Assets not owned by the enterprise must be removed from the network unless temporary access is granted by the IT business unit.
   2. Assets owned by the enterprise but not kept within the enterprise asset inventory must be added to the inventory.
2. Users are required to connect their enterprise assets to the enterprise network on a weekly basis, where practical.
3. Permanently air-gapped systems must be approved by IT.
4. IT must address unauthorized assets on a weekly basis at a minimum.
5. IT must choose to remove the unauthorized asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

### Usage

**In general, refer to the enterprise’s *Acceptable Use Policy*. The following can substitute until an appropriate policy is created:**

1. Users must handle all enterprise assets with care.
2. Bi-annual, or more frequent, verification of each enterprise asset must be completed in-person or remotely unless an exemption is authorized by supervisory management.
3. It is the responsibility of the enterprise asset owner to:
   1. Maintain control over the enterprise asset.
   2. Contact IT with any problems such as malfunctions, needed repairs, and underutilized equipment or in the event of equipment loss.

### Controlled Disposal

1. Enterprise assets to be decommissioned or retired must be returned to IT.
2. IT must make a copy of the user data, as needed.
3. IT will be responsible for the secure erasure of the primary memory storage device within the enterprise asset, where applicable.
4. IT will be responsible for updating the status of the enterprise asset within all enterprise management systems.
   1. IT must ensure that records are retained in compliance with the *Record Retention Policy*.
5. Document the removal of the enterprise asset from the enterprise within the asset inventory.

### Uncontrolled Disposal

1. All lost or stolen enterprise assets must be immediately reported to the appropriate business units, including IT, cybersecurity, and finance.
2. A report must be filed with law enforcement for all enterprise assets assumed stolen.
3. Lost and stolen enterprise assets must have their access to enterprise data revoked as soon as possible.
   1. The enterprise assets must also be removed from the inventory.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| IaaS | Infrastructure as a Service (IaaS) |
| ICS | Industrial Control System |
| IG | Implementation Group |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IT | Information Technology |
| MAC | Media Access Control |
| PaaS | Platform as a Service (PaaS) |
| SaaS | Software as a Service |

# 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 1: *Inventory and Control of Enterprise Assets*. Table 1 shows which IG1 Safeguards are covered by this policy as written.

Table 1 - Safeguards covered by IG1

| CIS Control | CIS Safeguard | Security Function | CIS Safeguard Title | CIS Safeguard Description | IG1 | IG2 | IG3 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1.1 | Identify | Establish and Maintain Detailed Enterprise Asset Inventory | Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise’s network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently. | X | X | X |
| 1 | 1.2 | Identify | Address Unauthorized Assets | Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset. | X | X | X |

# 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

National Institute of Standards and Technology®, Information Technology Laboratory, Computer Security Resource Center

<https://csrc.nist.gov/glossary/term/asset>

United States Department of Transportation, Federal Transit Administration

<https://www.transit.dot.gov/TAM/resources/assetinventory>