Acceptable Use  
Policy Template

**CIS Critical Security Controls**

**April 2023**

# Contents

[Contents 2](#_Toc132705896)

[Acknowledgments 3](#_Toc132705897)

[Introduction 4](#_Toc132705898)

[Purpose 4](#_Toc132705899)

[Scope 4](#_Toc132705900)

[Defining Enterprise Assets 4](#_Toc132705901)

[Acceptable Use Policy Topics 6](#_Toc132705902)

[Acceptable Use Policy Template 9](#_Toc132705903)

[Purpose 9](#_Toc132705904)

[Applicability 9](#_Toc132705905)

[Exceptions 9](#_Toc132705906)

[Policy 9](#_Toc132705907)

[Revision History 12](#_Toc132705908)

[Appendix A: Acronyms and Abbreviations 13](#_Toc132705909)

[Appendix B: Glossary 14](#_Toc132705910)

[Appendix C: Implementation Groups 16](#_Toc132705911)

[Appendix D: CIS Safeguards Mapping 17](#_Toc132705912)

[Appendix E: References and Resources 18](#_Toc132705913)

# 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:**

Tony Krzyzewski, SAM for Compliance Ltd  
Staffan Huslid, Truesec  
Diego Bolatti, Information Systems Engineer, Universidad Tecnológica Nacional (Argentina)   
Bryan Chou, CISSP, GSEC, GCED, GCIH  
Bryan Ferguson  
Gavin Willbond, SSS - IT Security Specialists  
Ken Muir  
Keala Asato  
Jon Matthies  
Robin Regnier, 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

Acceptable Use Policies often act as a terms and conditions document for employees. They are a cornerstone of an information security policy suite. Users will typically be required to read the document, confirm their understanding, and sign before they are given access to enterprise assets, data, and other resources. These user agreements are typically meant to apply throughout the enterprise, but it is sometimes necessary for project-specific and business unit-specific agreements to exist. The rules defined within this document must be regularly updated to meet the enterprise’s needs, and regularly enforced. Acceptable Use Policies help to reduce risk and educate users on current company policy. Therefore, they need to be written in such a way as to be easy to understand and follow by all readers, regardless of their level of technical expertise.

## Purpose

The CIS Critical Security Controls® (CIS Controls®) recommends several policies that an enterprise should have in place as foundational elements of its cybersecurity program. The CIS Controls Information Security Policy Working Group worked to develop policies to support the CIS Controls. Once the initial scope of the Working Group was completed, the Working Group recommended that an Acceptable Use Policy template also be created. This policy template exists outside the typical topics covered within the CIS Controls, since the CIS Controls do not address acceptable use. If desired, enterprises are encouraged to use this policy template in whole or in part. The specific content of an Acceptable Use Policy varies widely. With that said, it’s often considered best practice to include what a user is permitted to do with enterprise data, how the enterprise assets can be used, and how enterprise data can be transmitted to other parties.

## 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). [Appendix D](#_Appendix_D:_CIS) notes that there are 0 CIS Safeguards within this Policy mapped to the CIS Controls. 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. Depending on an enterprise’s sector or mission, other policy statements may also need to be added or removed.

## Defining Enterprise Assets

There are many types of enterprise assets that can exist in an enterprise. Many of them will need to be covered by an Acceptable Use Policy, but there will be situations where this is not be possible. For instance, users outside the information technology (IT) business unit will rarely need to enter the server room and manage servers, meaning servers may not need to be covered by the more general Acceptable Use Policy. For the purposes of this document and in the 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

Graphical user interface, application

Description automatically generated

Figure . Enterprise assets, as defined in CIS Controls v8

# Acceptable Use Policy Topics

The CIS Information Security Policy Templates generally follow a lifecycle model, but that is not possible within this policy template. An Acceptable Use Policy simply informs employees as to how they are allowed to use the information technology (IT) assets their enterprise has provided them in order to perform their job. Essentially a list of DOs and DON’Ts, or “Acceptable Use” and “Unacceptable Use”. The actual content of an *Acceptable Use Policy* will vary, but generally it contains best practice for the following topics to be covered:

Diagram

Description automatically generated

* **Acceptable Use** – Actions that employees may perform with their enterprise assets.
* **Prohibited Use** – Actions that employees must not perform with their enterprise assets.
* **Personal Use** – Restrictions around the usage of enterprise assets for personal affairs.
* **Privacy Expectations** – Descriptions of the level of privacy that users can expect while working with their enterprise assets.
* **Reporting Violations** – Methods to report violations of the enterprise Acceptable Use Policy, and other enterprise policies.
* **Remote Work** – Policies for users working from their homes rather than the office or assigned duty station.
* **Bring Your Own Device** – Statements restricting or enabling the usage of personal devices for work activities.

**Acceptable Use**

This topic area should describe the manner in which users are authorized to use their enterprise assets, data, and other resources. Specific types of assets covered by the Acceptable Use Policy should be listed, such as workstations, mobile devices, and laptops. Specific applications may also be covered, especially browsers, email, contacts, and calendar. Acceptable methods of handling enterprise data should be discussed, which should specifically call out intellectual property. Finally, policies relating to social media may be placed here, or in the *Prohibited Use* topic area.

**Prohibited Use**

Actions that you do not want your users to take with their enterprise assets can be placed within this topic area. Many of the items listed here could also be stated in a different way within the *Acceptable Use* topic area. The number of policy statements listed within *Prohibited Use* may be a good deal larger than under *Acceptable Use*. Although each enterprise will vary as to what specifically should be placed here, example topics include: usage of cloud storage and file sharing services, shadow IT, connecting enterprise assets to other networks not owned by the enterprise, and use of enterprise assets on social media and representing the enterprise to the public more generally. When in doubt, it may be prudent to over-specify prohibited actions and modify the Acceptable Use Policy over time after experience is gained. With that said, policy writers should not place a multitude of prohibited activities within the Acceptable Use Policy that are not regularly enforced.

**Personal Use of Enterprise Assets**

Personal use of enterprise assets can be a challenging topic. It’s easy to imagine a spectrum of personal use, starting from “no personal use of enterprise assets” ranging to “users can do whatever they want with enterprise assets”. Most enterprises will fall somewhere in the middle of that spectrum. A clear, well written policy can help users understand what is, and is not appropriate, with different classes of enterprise assets. For instance, users may be issued enterprise phones, and can perform a variety of personal tasks on those devices, yet a different set of rules may apply to laptops. Personal usage of enterprise assets are not the only topics that need to be considered. How users access enterprise resources and handle enterprise data on personal devices can have a massive security impact on the overall enterprise. In part due to this fact, bring you own device (BYOD) is further broken out into a separate topic area within this policy template.

At the very least, *Personal Use* policy statements should cover rules for users visiting websites and checking personal email accounts on enterprise assets. A common turn of phrase found in many acceptable use policies is “limited personal use.” There is no 100% agreed upon definition of this term, and enterprises should work to define what limited personal use means for them if it will be used. As users are extremely likely to check their email and visit personal sites using enterprise assets, regardless of enterprise policy, a realistic definition is needed. Other topics include using personal accounts across an entire device, storing enterprise data in personal cloud platforms. Browser synching and browser profiles should also be considered, since unsafe websites and applications the user visits in their personal time on personal devices may propagate back to enterprise assets. Usage of password managers can also be discussed, especially if the enterprise does not provide an enterprise-authorized password manager.

**Privacy Expectations**

Users should be made aware that on enterprise assets, users should expect no degree of personal privacy. This means that all data stored, and all communications originating from enterprise assets are owned by the enterprise and may be monitored and reviewed. While best practice is to keep personal data or communications on personal devices and off the enterprise network, some enterprises may allow for shared use of enterprise assets and BYOD.

**Reporting Violations**

Enterprises should clearly define how users can report violations of the Acceptable Use Policy, other enterprise policies, and any potential signs of a data breach within the enterprise. This should be incorporated into the enterprise’s Cybersecurity Awareness Training Program. Users should be informed that self-reported violations will not have repercussion in order to ensure this information is made available to the enterprise.

**Bring Your Own Device (BYOD)**

BYOD is the practice of enterprise users leveraging their personal devices for enterprise tasks. Most commonly, these devices are either smart phones or laptops. There are multiple ways to implement BYOD, such as placing the device completely under enterprise management control, using a virtual private network (VPN) to obtain an internal internet protocol (IP) address, isolating BYOD devices into restricted networks, or simply allowing a device to connect to enterprise cloud services via an app on the device. Enterprises should work to protect their information on personal devices and ensure other applications are not accessing sensitive or confidential material. Note that this Acceptable Use Policy alone is insufficient to create a BYOD policy and enterprises are encouraged to develop their own robust BYOD policies to cover situations and threats unique to them. More advanced enterprises, such as those self-classifying as CIS Implementation Group (IG) IG2 and IG3 should be using mobile device management and enterprise mobility management tools to enable BYOD. For additional guidance of using the CIS Controls for mobile devices, please see the [CIS Controls Mobile Companion Guide](https://www.cisecurity.org/insights/white-papers/cis-controls-mobile-companion-guide-2).

**Remote Work**

Remote working occurs whenever enterprise users work from a location outside of the enterprise’s premises, accessing information whether in hardcopy or electronically via enterprise equipment. Remote working environments include those referred to as “teleworking”, “telecommuting”, “flexible workplace”, “virtual work environments" and “remote maintenance”. The enterprise should inform users that it does not matter where they are working, this Acceptable Use Policy applies. Enterprises should encourage users to take extra security precautions when working remotely, including allowing other people into the remote working location to potentially have access or view enterprise data. Note that this Acceptable Use Policy alone is insufficient to create a comprehensive remote work policy and enterprises are encouraged to develop robust remote work programs.

# Acceptable Use Policy Template

## Purpose

This *Acceptable Use Policy* acts as an agreement between the enterprise and the user receiving Information Technology (IT) assets. Assets are defined as anything that has value to an organization, including, but not limited to, another organization, person, computing device, IT system, IT network, 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). This *Acceptable Use Policy* defines permitted usage of these assets, as well as restricted actions that users must not take in order to reduce risk to the enterprise.

## Applicability

This policy is meant to apply to all users within the enterprise who receive and utilize enterprise assets, which includes all members of the workforce (both on-site and remote), third-party vendors, contractors, service providers, consultants, or any other individual that operates an enterprise asset. It is the user’s responsibility to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand the enterprise’s Information Security Policy and its associated standards. Users who find the policy statements within this document to be unclear are encouraged to reach out to IT in order to clarify any remaining ambiguities.

## Exceptions

Exceptions to this policy are likely to occur. Exception requests may occur for a variety of reasons, but generally employees will need to use enterprise IT assets in a manner that is inconsistent with policy. As an example, it’s common to need to connect a personal device to the enterprise network, or place enterprise data in the possession of a third-party contractor. All exception requests 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.

All exceptions must be approved by a manager authorized to approve the exception.

## Policy

**User Responsibilities**

1. Users must only use approved technology and services.
2. All enterprise assets are on loan to users so that essential job functions may be performed.
3. Upon separation from the enterprise or contract termination, all supplied IT assets, and the associated data must be returned by the user.
4. Users must secure the physical environment around their workstation and lock their computers when stepping away.
5. Users must ensure that Personally Identifiable Information (PII), confidential, and any sensitive data that may be covered by government or other regulation, is not readily available or accessible on their desks or within their workspace.
6. All users must take appropriate care to protect information, systems and related assets within their custody or care from loss, damage, or harm.
   1. Lost or damaged equipment must be reported to IT as soon as practical.
7. Users must store their passwords in a secure manner.
   1. Approved password managers must be used to store passwords digitally.
8. Users-assigned accounts must only access assets, operating systems, applications, files, and data to which they have been granted access. The ability to inadvertently read, execute, modify, delete, or copy data does not imply permission to do so.
9. Only authorized users are permitted to post content or create the impression that they are representing, stating opinions, or otherwise making statements on behalf of the enterprise on social networking sites, blogs, or other internet sites.
10. Users must keep knowledge about information and information systems gained during employment confidential and confidentiality must be maintained after employment ceases.

**Prohibited Use**

1. Only approved and authorized devices may be connected to networks owned or managed by the enterprise. This includes portable ender-user devices, removable devices (e.g., USB sticks) and personally-owned devices.
2. Users must not share their passwords with others or allow the use of their account by others.
   1. Users are responsible for all activity originating from their usernames and accounts.
3. Users must not circumvent user authentication mechanisms or the security of any user account or information system asset.
4. Users must not install software, hardware, or modify system configuration settings on any enterprise asset, unless explicitly permitted by the user’s role and responsibility.
5. Users must not engage in any activity with the intent to disrupt enterprise assets or networks.
   1. Users must not perform any form of network monitoring, port scanning or security scanning unless this activity is a part of the individual's normal job and is formally authorized.
6. Users must not leverage enterprise assets for personal economic gain.
7. Users must not leverage the “Remember Me” or “Remember my Password” function inside of a browser.

**Expectations of Privacy**

1. When using enterprise resources, the user shall have no expectation of privacy. Access and use of the Internet, including communication by e-mail and instant messaging and the content thereof, are not confidential, except in certain limited cases recognized by law.
2. The enterprise reserves the right to monitor, access, and disclose all information generated and actions performed using enterprise IT assets. Files, messages (including attachments), and logs may be retained and used as evidence in litigation, audits, and investigations.

**Personal Use**

1. Users are permitted limited personal use of enterprise assets, such as visiting websites and checking personal email accounts.
   1. Users may access web-based personal password managers on enterprise assets. Local installation of a password manager must be approved by IT.
      1. Users must not store enterprise passwords in personal password managers.
   2. Users must not leverage browser synch or browser profiles that will move a user’s browser history from a personal device to an enterprise asset (or vice versa).
2. Users must not use personally-owned accounts (e.g., Apple ID, Google Account, Microsoft Account) for device-wide accounts (e.g., Android, iOS, Windows) on enterprise devices unless permitted by the enterprise.
   1. Users must work with IT to create enterprise-specific accounts for required assets and third-party services, such as creating an enterprise-owned Apple ID for an Apple device.
3. Users must not use enterprise license keys on personal devices unless authorized by the enterprise.
4. Enterprise data must not be stored on non-enterprise, personal cloud provider platforms (e.g., Google Drive, Microsoft OneDrive, Dropbox).

**Reporting Violations**

1. Users who are aware of any event which threatens the availability, integrity or confidentiality of enterprise data, or which breaches any standard, policy, procedure, or any associated requirement, or is contrary to law, must immediately contact IT or their immediate manager.

**Remote Work**

1. All enterprise work must be performed on enterprise-approved assets.
2. All enterprise data must be stored on approved enterprise assets.
3. Users must not connect enterprise assets to open, unencrypted WiFi networks.
4. Users must be aware of their surroundings when working remotely to ensure others are not shoulder surfing or viewing sensitive material.

**Bring Your Own Device**

1. Personal devices must not be connected to the enterprise network without formal authorization.
2. Enterprise data must not be stored on personal devices without formal authorization.
3. Users leveraging their personal device to store enterprise data may have their device completely wiped. Reasons for device wipe may include:
   1. Lost / stolen device.
   2. Termination of user’s employment.
   3. Compromised / hacked account or device.

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

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Revision Date | Revision Description | Name |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Appendix A: Acronyms and Abbreviations

|  |  |
| --- | --- |
| BYOD | Bring your own device |
| CIS | Center for Internet Security |
| CIS Controls | Center for Internet Security Critical Security Controls |
| ICS | Industrial controls systems |
| IG | Implementation Group |
| IoT | Internet of Things |
| IP | Internet protocol |
| IT | Information Technology |
| PII | Personally Identifiable Information |
| VPN | Virtual Private Network |

# 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 individual 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 does not contain any mappings to the CIS Controls.

Table - Safeguards covered by IG1

|  |  |  |  |
| --- | --- | --- | --- |
| CIS Control | Policy Statement | CIS Safeguard | CIS Safeguard  Description |
| N/A | N/A | N/A | N/A |
| N/A | N/A | N/A | N/A |
| N/A | N/A | N/A | N/A |

# Appendix E: References and Resources

Center for Internet Security®

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

CIS Critical Security Controls®

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