Security Awareness
Skills Training
Policy Template

**CIS Critical Security Controls**

**March 2023**

# Contents

[Contents 2](#_Toc128322011)

[Acknowledgments 3](#_Toc128322012)

[Introduction 4](#_Toc128322013)

[Purpose 4](#_Toc128322014)

[Types of Training 4](#_Toc128322015)

[Scope 4](#_Toc128322016)

[Security Awareness Training Lifecycle 6](#_Toc128322017)

[Security Awareness Training Policy Template 9](#_Toc128322018)

[Purpose 9](#_Toc128322019)

[Responsibility 9](#_Toc128322020)

[Exceptions 9](#_Toc128322021)

[Policy 9](#_Toc128322022)

[Revision History 11](#_Toc128322023)

[Appendix A: Acronyms and Abbreviations 12](#_Toc128322024)

[Appendix B: Glossary 13](#_Toc128322025)

[Appendix C: Implementation Groups 16](#_Toc128322026)

[Appendix D: CIS Safeguards Mapping 17](#_Toc128322027)

[Appendix E: References and Resources 19](#_Toc128322028)

# 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
Ginger Anderson, CIS
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

The actions of employees, contractors, and other users play a critical part in the success or failure of an enterprise’s security program. It is sometimes easier for an attacker to entice a user to click a link or open an email attachment to install malware in order to get into an enterprise, than to find a network exploit to do it directly. Users themselves, both intentionally and unintentionally, can cause incidents as a result of mishandling sensitive data, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, using weak passwords, or using the same password they use on public sites. No security program can effectively address cyber risk without a means to address this fundamental human vulnerability.

## Purpose

The Center for Internet Security® (CIS®) recommends several policies that an enterprise should have in place. This *Security Awareness Training Policy* is meant as a “jumping off point” for enterprises that need help drafting their own policy. Enterprises are encouraged to use this policy template in whole or in part. With that said, there are multiple decision points and areas that must be tailored to an enterprise’s specific needs, such as the best way to deliver training and educate your users, and which specific topics to cover.

In CIS Controls v8, Control 14 states:

**Control 14 – Security Awareness and Skills Training –** A Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

To support this Safeguard, it is important for an enterprise to develop a robust security awareness training program. An effective security awareness training program should not just be a canned, once-a-year training video coupled with regular phishing testing. While annual training is needed, there should also be more frequent, topical messages and notifications about security. This might include messages about: strong password-use that coincides with a media report of password dump, the rise of phishing during tax time, or increased awareness of malicious package delivery emails during the holidays. This document supports the development of a process for managing enterprise assets and the implementation of Safeguards in this CIS Control.

## Types of Training

There are many methods that can be used to educate users on cybersecurity. A major decision point includes whether training will be provided by a person or if users will be taking training on their own time via digital means. These options are not mutually exclusive, and a combination of these methods may be leveraged. Additionally, ancillary methods such as posters, signs, and email reminders may be used to remind users of their information security responsibilities.

## Scope

This *Security Awareness Training Policy* is divided into multiple sections based on how enterprise will practically plan, develop, and deliver training. 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). Depending on an enterprise’s sector or mission, other policy statements may also need to be added or removed. 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.

# Security Awareness Training Lifecycle

Not all security trainings are made equal. The enterprise that takes the time and resources to develop and provide high quality security training to their users will have the best chance at defending themselves from some of the most pernicious and persistent threats. Shown below in Figure 1 are the high-level aspects of the *Security Awareness Training Lifecycle*, followed by a detailed description of what each step entails. This is not the only way to run a program, but this can act as a foundation to build your own program upon.



Figure 1. Security Awareness Training Lifecycle

* **Assess** – Perform requirements gathering and explore the appropriate methods for providing training.
* **Develop** – Build out a training program for your enterprise, to include purchasing an existing tool, or creating tailored educational material.
* **Educate** – Deliver cybersecurity training content to users across the enterprise.
* **Validate** – Ensure that users are benefiting from the training and provide supplemental support to bolster training goals.

**Assess**

Creating a security awareness program from scratch will take time and planning. Enterprises will approach this task with different starting points, styles, and goals in mind. At a high level, there are a few points that should be considered for all programs. That includes requirements gathering, training delivery method, and whether to use external tools and resources. *NIST SP 800-50: Building an Information Technology Security Awareness and Training Program[[1]](#footnote-1)* can act as a comprehensive guide to this subject. Generally, enterprises are encouraged to create or use broad training programs that are then tailored to specific industries, roles, and employees.

Requirements gathering for security awareness training ultimately comes down to why an enterprise wants or needs training. The answer may simply be that the enterprise is required to by law or policy. Understanding your requirements ensures that an enterprise is fulfilling their obligations (legal, or otherwise), and can assist employees in getting the most out of the training they are receiving. This can include making the training contextually relevant, in any spoken or written languages the employees need, and address threats that may be unique or more applicable to a vertical.

One of the first items an enterprise should consider is how the training will be delivered. In-person training is generally considered more effective than online training, but it is often more expensive to have a trainer physically at an office, but the particulars vary. Collecting all employees into a single building, office, auditorium can be expensive. The costs for an experienced external trainer or guest speaker can be expensive, so it’s commonplace for enterprises with internal cybersecurity expertise to leverage an employee with cybersecurity expertise to deliver the training.

Online training is often viewed as a resource-efficient method of providing training. Many types of online training exist, including trivia and tests, videos, games, and scenario-based experiences. These methods of training may work fantastically for an enterprise, but they are rarely targeted to a specific enterprise’s needs since much of the material is developed to be as broad and applicable as possible for many types of customers. A hybrid solution is sometimes used, where employees must view presentations but also complete an online component such as a test.

**Develop**

This part of the process assists enterprises in developing a training program that meets the enterprise’s training requirements. Training must then be either developed or acquired that meets the requirements. This often occurs by purchasing a product after performing market research, developing training internally, or a hybrid of these two approaches. Many security awareness training modules are available freely online, alongside videos on sites such as YouTube and Vimeo. Decisions must also be made such as how often training will be delivered, and when supplemental training will be required. At the very least, CIS recommends training be performed at the time of user onboarding and then at least annually. The content of the security awareness training program must be updated when new threats affecting enterprise are identified.

**Educate**

In this phase, training is delivered to all enterprise users that have access to enterprise systems and information. This should be performed in accordance with the cadence dictated by internal policy and any outside requirements previously identified. For instance, if a security framework used by the enterprise recommends annual training on specific topics. Users attending and completing the training should be tracked by Information Technology (IT) or other relevant business unit (e.g., Information Security Office) to ensure that the required users received training and that the enterprise’s obligations are met.

The content of the training should meet requirements identified during the assessment phase. The CIS Controls suggests a variety of topics that an IG1 organization should train their users on, such as multi-factor authentication, how to securely handle data, and report suspected security issues to the proper in-house authority. Additionally, the training should include any necessary information needed to make security-aware decisions on the technology and applications used in the enterprise. This could include things like understanding what a dialog box from anti-malware program installed on your endpoints is supposed to look like. There are also topics that are outside of the scope of the CIS Controls that are commonly discussed, such as physical security topics. This includes policies and procedures relating to physical access to include entering and leaving the office, use of badges and IDs, physical security requirements for server rooms, and challenging unknown persons in a restricted area.

**Validate**

Users may not be thrilled to regularly attend cybersecurity training, yet it is often the job of IT, or other relevant business unit (e.g., Information Security Office), to ensure that all required users attendedtraining. Additionally, this training generally must be completed by users within a defined timeframe. Some enterprises go so far as to verify that the training was completed within realistic bounds such as is the case when a user completes the entire training program in under a minute. This step in the phase focuses on verifying that education obligations are met, alongside suggesting additional measures an enterprise may want to take to ensure users are learning from the training. For instance, some organizations may want to move past quarterly or annual training and perform periodic phishing tests of their own users. Many vendors can offer this service at minimal cost. Finally, tabletop exercises or scenario-based training may be offered from time to time to allow users to flex their cybersecurity knowledge, instead of just passively listening or viewing the content.

Once all applicable users have completed the yearly training, the enterprise must then embark on updating the training materials. There’s a variety of reasons why this would need to happen such as enterprise policies changing from time to time. Users need to be made aware of these changes. Technology updates will be made to the enterprise, such as receiving a new type of anti-malware application or email filter, and users will need to understand their responsibilities and how to effectively use these new systems. Another reason training may need to be updated is new and emerging threats. From time to time, a new type of attack or class of attacks will arise, such as what happened within the last decade with ransomware and destructive malware.

# Security Awareness Training Policy Template

## Purpose

A modern cybersecurity program cannot be put into place without ample attention given to security awareness training. This includes designing a robust program that is properly developed, implemented, and updated. The *Security Awareness Training Policy* provides the processes and procedures for this program.

## Responsibility

The IT business unit has the primary responsibility for planning, developing, and updating the cybersecurity awareness training program. The education aspect may be performed by the IT business unit or others they deem fit to provide the training. With that said, all employees and users have a responsibility to implement the concepts taught within the security awareness program.

## Exceptions

Exceptions to this policy are likely to occur. 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.

## Policy

**Assess**

There are no IG1 safeguards that support this portion of the security awareness training process.

**Develop**

1. A program for performing security awareness training must be established.
2. This process must be documented and approved.

**Educate**

1. Users must receive security awareness training, at a minimum, on an annual basis.
2. All new users must receive cybersecurity awareness training before being granted access to enterprise assets.
3. Users must be trained on how to recognize social engineering attacks.
4. Users must be trained on best practices for authentication in the enterprise. Users must be trained on best practices for handling enterprise data.
	1. Training must be included on the following subjects as it pertains to the enterprise’s *Data Management Policy*:
		1. Identifying sensitive data
		2. Storing sensitive data
		3. Transferring sensitive data
		4. Archiving sensitive data
		5. Destroying sensitive data
		6. Any legal and / or regulatory obligations of the above.
	2. Clear screen and clean desk best practices must be included in the training.
		1. Timeframes for automatic session locking for enterprise assets are contained within the *Secure Configuration Management Policy*.
5. Users must be trained on the causes of unintentional data exposure in the enterprise.
6. Users must be trained on how to recognize and report security incidents.
7. Users must be trained on how to identify and report if their enterprise assets are missing security updates.
8. Users must be trained on the dangers of connecting to and transmitting enterprise data over insecure networks.

**Update**

1. The content of the security awareness training program must be reviewed and updated annually, or when significant changes to the enterprise occur.

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 |
| IG | Implementation Group |
| IT | Information Technology |

# 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) |
| Breach | The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses sensitive or confidential information; or an authorized user accesses sensitive or confidential information for other than authorized purposes.Source: *Modified from* [Breach - Glossary | CSRC (nist.gov)](https://csrc.nist.gov/glossary/term/breach) |
| 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). |
| Data Exposure  | An unintentional data breach. Source: CIS |
| 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 |
| 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 |
| Multifactor Authentication | Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password), something you have (e.g., cryptographic identification device, token), or something you are (e.g., biometric). Source: [NIST SP 800-172](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf) |
| 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 |
| Phishing | A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.Source: [IETF RFC 4949 Ver 2](https://tools.ietf.org/html/rfc4949) |
| Pretexting | Part of a social engineering attack that involves inventing a scenario to convince the victim to divulge information that should not be divulged. The purpose of pretexting is to convince the victim of the legitimacy of the communication. The method of this type of attack can be through any communication method or medium. Source: CIS  |
| 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 |
| Tailgating | A physical security issue where an individual follows another into a secured area without properly authenticating or following established protocols for entering the area. Source: CIS |
| 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 |

# 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 14: *Security Awareness and Skills Training*. Table 1 shows which IG1 Safeguards are covered by this policy as written.

Table - Safeguards covered by IG1

|  |  |  |  |
| --- | --- | --- | --- |
| CIS Control | Policy Statement | CIS Safeguard | CIS Safeguard Description |
| 14.1 | Develop 1, 2Update 1  | Establish and Maintain a Security Awareness Program | Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise’s workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard. |
| 14.2 | Educate 3 | Train Workforce Members to Recognize Social Engineering Attacks | Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.  |
| 14.3 | Educate 4 | Train Workforce Members on Authentication Best Practices | Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management. |
| 14.4 | Educate 5 | Train Workforce on Data Handling Best Practices | Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely. |
| 14.5 | Educate 6  | Train Workforce Members on Causes of Unintentional Data Exposure | Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences. |
| 14.6 | Educate 7  | Train Workforce Members on Recognizing and Reporting Security Incidents | Train workforce members to be able to recognize a potential incident and be able to report such an incident. |
| 14.7 | Educate 8  | Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates | Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools. |
| 14.8  | Educate 9  | Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks | Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure. |
| 17.3 | Educate 7 | Establish and Maintain an Enterprise Process for Reporting Incidents | Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard. |

# Appendix E: References and Resources

Center for Internet Security®

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

CIS Critical Security Controls®

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

SANS: Ouch! Newsletters Security awareness newsletter
[SANS OUCH!](https://www.sans.org/newsletters/ouch/)

NIST SP 800-50: Building an Information Technology Security Awareness and Training Program
<https://csrc.nist.gov/publications/detail/sp/800-50/final>

SANS: Internet Storm Center® Monitors the level of malicious activity on the internet

YouTube: Social Engineering Attacks (Professor Messer)
<https://www.youtube.com/watch?v=QUgLxll_P58>

NIST: You’ve Been Phished! videos Educational videos
<https://www.nist.gov/video/youve-been-phished>

Berkeley: The Phish Tank Phishing examples
<https://security.berkeley.edu/resources/phish-tank>

MS-ISAC® Newsletter Subscription Newsletters, advisories, and webinars on cybersecurity threats
<https://learn.cisecurity.org/ms-isac-subscription>

MS-ISAC® Cybersecurity Awareness Toolkit
<https://www.cisecurity.org/ms-isac/ms-isac-toolkit>

Federal Virtual Training Environment (FedVTE) Online Courses
<https://fedvte.usalearning.gov/>

National Cyber Security Alliance (NCSA®) Nonprofit promoting cybersecurity awareness and education
<https://staysafeonline.org/>

YouTube: StaySafeOnline.org
<https://www.youtube.com/user/StaySafeOnline1/videos>

1. <https://csrc.nist.gov/publications/detail/sp/800-50/final> [↑](#footnote-ref-1)