UTAH SYSTEM OF HIGHER EDUCATION

MEMORANDUM

November 18, 2022

Revision to Policy R345, *Information Technology Resource Security*

The chief information officers (CIOs) at degree-granting institutions and technical colleges have reviewed Board Policy R345, *Information Technology Resource Security*. They have proposed updates to bring this policy in line with current standards. Steve Hess leads the group of CIOs. Steve Hess, Ph.D., is the chief information officer (CIO) of the University of Utah and also serves as the CIO of the Utah System of Higher Education.

These proposed policy revisions are necessary to bring information technology security standards up to date. This revision relies heavily on the Center for Internet Security Critical Security Controls. The Center for Internet Security (CIS) is a globally recognized non-profit organization responsible for developing internet security controls and benchmarks and setting best practices for securing IT systems and data. The CIS Critical Security Controls are a prioritized set of safeguards to mitigate the most prevalent cyber-attacks against systems and networks. CIS Critical Security Controls are developed around controls implementation groups designed to assess appropriate levels of controls for organizations with similar risk profiles and resources. This enables all institutions to work towards appropriate levels of controls.

This policy revision relates to the Board's Strategic Plan priority of Affordability and the strategy to expand shared services. Establishing appropriate policies related to information technology is a core enabler that is foundational in moving forward with additional shared services related to cybersecurity. This policy revision is also foundational in supporting the systemwide budget priority of cybersecurity. This policy revision also supports the Board's governance role to monitor, control, and supervise the system of higher education.

Commissioner's Recommendation

The Commissioner recommends the Board approve the proposed revisions to Board Policy R345, *Information Technology Resource Security*, including the references to the Center for Internet Security Critical Security Controls.

Attachments

Center for Internet Security®

CIS Controls®

CIS Controls

Version 8

CIS Controls Version 8

Acknowledgments

CIS would like to thank the many security experts who volunteer their time and talent to support the 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.

Creative Commons License

May 2021

Contents

Glossary

Administrator accounts	Dedicated accounts with escalated privileges and used for managing aspects of a computer, domain, or the whole enterprise information technology infrastructure. Common administrator account subtypes include root accounts, local administrator and domain administrator accounts, and network or security appliance administrator accounts.
Application	A program, or group of programs, hosted on enterprise assets and designed for end-users. Applications are considered a software asset in this document. Examples include web, database, cloud-based, and mobile applications.
Authentication systems	A system or mechanism used to identify a user through associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system, user directory service, or within an authentication server. Examples of authentication systems can include active directory, Multi-Factor Authentication (MFA), biometrics, and tokens.
Authorization systems	A system or mechanism used to determine access levels or user/client privileges related to system resources including files, services, computer programs, data, and application features. An authorization system grants or denies access to a resource based on the user's identity. Examples of authorization systems can include active directory, access control lists, and role-based access control lists.
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).
Database	Organized collection of data, generally stored and accessed electronically from a computer system. Databases can reside remotely or on-site. Database Management Systems (DMSs) are used to administer databases, and are not considered part of a database for this document.
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.
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.
Externally-exposed enterprise assets	Refers to enterprise assets that are public facing and discoverable through domain name system reconnaissance and network scanning from the public internet outside of the enterprise's network.
Internal enterprise assets	Refers to non-public facing enterprise assets that can only be identified through network scans and reconnaissance from within an enterprise's network through authorized authenticated or unauthenticated access.

Library	Pre-written code, classes, procedures, scripts, configuration data, and more, used to develop software programs and applications. It is designed to assist both the programmer and the programming language compiler in building and executing software.
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.
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.
Network infrastructure	Refers to all of the resources of a network that make network or internet connectivity, management, business operations, and communication possible. It consists of hardware and software, systems and devices, and it enables computing and communication between users, services, applications, and processes. Network infrastructure can be cloud, physical, or virtual.
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.
Operating system	System software on enterprise assets that manages computer hardware and software resources, and provides common services for programs. Operating systems are considered a software asset and can be single- and multi-tasking, single- and multi-user, distributed, templated, embedded, real-time, and library.
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.
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 smartphones and tablets, all of which are a subset of enterprise assets.
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.
Remote file systems	Enable an application that runs on an enterprise asset to access files stored on a different asset. Remote file systems often make other resources, such as remote non-computing devices, accessible from an asset. The remote file access takes place using some form of local area network, wide area network, point-to-point link, or other communication mechanism. These file systems are often referred to as network file systems or distributed file systems.

Removable media	Any type of storage device that can be removed from a computer while the system is running and allows data to be moved from one system to another. Examples of removable media include compact discs (CDs), digital versatile discs (DVDs) and Blu-ray discs, tape backups, as well as diskettes and universal serial bus (USB) drives.
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.
Service accounts	A dedicated account with escalated privileges used for running applications and other processes. Service accounts may also be created just to own data and configuration files. They are not intended to be used by people, except for performing administrative operations.
Services	Refers to a software functionality or a set of software functionalities, such as the retrieval of specified information or the execution of a set of operations. Services provide a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and based on the identity of the requestor per the enterprise's usage policies.
Social engineering	Refers to a broad range of malicious activities accomplished through human interactions on various platforms, such as email or phone. It relies on psychological manipulation to trick users into making security mistakes or giving away sensitive information.
Software assets	Also referred to as software in this document, these are the programs and other operating information used within an enterprise asset. Software assets include operating systems and applications.
User accounts	An identity created for a person in a computer or computing system. For the purpose of this document, user accounts refer to "standard" or "interactive" user accounts with limited privileges and are used for general tasks such as reading email and surfing the web. User accounts with escalated privileges are covered under administrator accounts.
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.

Acronyms and Abbreviations

AAA	Authentication, Authorization, and Auditing
ACL	Access Control List
AD	Active Directory
AoC	Attestation of Compliance
API	Application Programming Interface
BEC	Business Email Compromise
C2	Command and Control
CCE	Common Configuration Enumeration
CDM	Community Defense Model
CIA	Confidentiality, Integrity, and Availability
CIS	Center for Internet Security
CIS-CAT	CIS Configuration Assessment Tool
COTS	Commercial off-the-Shelf
CPE	Common Platform Enumeration
CREST	Council of Registered Security Testers
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DBIR	Data Breach Investigations Report
DEP	Data Execution Prevention
DG	Development Group
DHCP	Dynamic Host Configuration Protocol
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DMS	Database Management System
DNS	Domain Name System
DPI	Deep Packet Inspection
EDR	Endpoint Detection and Response
EOL	End of Life
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Modernization Act
GRC	Governance Risk and Compliance
HECVAT	Higher Education Community Vendor Assessment Toolkit
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IDS	Intrusion Detection System
IG	Implementation Group
IOCs	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
LotL	Living off the Land
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge®
MS-ISAC	Multi-State Information Sharing and Analysis Center
NaaS	Network-as-a-Service
NCSA	National Cyber Security Alliance
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OS	Operating System
OSS	Open Source Software
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PAM	Privileged Access Management
PCI	Payment Card Industry

SaaS	Software as a Service
SAFECode	Software Assurance Forum for Excellence in Code
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SIEM	Security Information and Event Management
SIP	System Integrity Protection
SMS	Short Messaging Service
SOC	Security Operations Center
SOC 2	Service Organization Control 2
SPAM	Something Posing as Mail
SPF	Sender Policy Framework
SQL	Structured Query Language
SSDF	Secure Software Development Framework
SSH	Secure Shell
SSO	Single Sign-On
Telnet	Teletype Network
TLS	Transport Layer Security
TTPs	Tactics, Techniques, and Procedures
U.K.	United Kingdom
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WDEG	Windows Defender Exploit Guard
WPA2	Wi-Fi Protected Access 2
XCCDF	Extensible Configuration Checklist Description Format

Overview

Overview

Introduction

The CIS Controls® started as a simple grassroots activity to identify the most common and important real-world cyber-attacks that affect enterprises every day, translate that knowledge and experience into positive, constructive action for defenders, and then share that information with a wider audience. The original goals were modest—to help people and enterprises focus their attention and get started on the most important steps to defend themselves from the attacks that really mattered.

Led by the Center for Internet Security® (CIS®), the CIS Controls have matured into an international community of volunteer individuals and institutions that:

- Share insights into attacks and attackers, identify root causes, and translate that into classes of defensive action
- Create and share tools, working aids, and stories of adoption and problem-solving
- Map the CIS Controls to regulatory and compliance frameworks in order to ensure alignment and bring collective priority and focus to them
- Identify common problems and barriers (like initial assessment and implementation roadmaps), and solve them as a community

The CIS Controls reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals), with every role (threat responders and analysts, technologists, information technology (IT) operators and defenders, vulnerability-finders, tool makers, solution providers, users, policy-makers, auditors, etc.), and across many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT, etc.), who have banded together to create, adopt, and support the CIS Controls.

Evolution of the CIS Controls

The CIS Controls started like many similar activities; we gathered experts together, and shared and argued until we reached an agreement. This can be very valuable, depending on the people at the table and their experience. Through documenting and sharing the output, all enterprises can benefit from the work of people they cannot hire or even meet. You can improve the outcome (and your confidence in it) through selecting experts that represent a wide range of knowledge, bringing consistency to the process, and ensuring use of the best-available information (especially about attacks). In the end, you are still depending on the good judgment of a relatively small group of people, captured in an informal and narrative way.

At CIS, we have been on a multi-year path to bring more data, rigor, and transparency to the process of best practice recommendations (the CIS Benchmarks™ and the CIS Controls). All of these elements are essential to the maturation of a science to underlie cyber defense; and, all are necessary to allow the tailoring and "negotiation" of security actions applicable in specific cases, and as required through specific security frameworks, regulations, and similar oversight schemes.

In the earliest versions of the CIS Controls, we used a standard list of publicly known attacks as a simple and informal test of the usefulness of specific recommendations. Starting in 2013, we worked with the Verizon Data Breach Investigations Report (DBIR) team to map the results of their large-scale data analysis directly to the CIS Controls, as a way to match their summaries of attacks into a standard program for defensive improvement.

CIS has recently released the **Community Defense Model (CDM)**, which is our most data-driven approach so far. In its initial version, the CDM looks at the conclusions from the most recent Verizon DBIR, along with data from the **Multi-State Information Sharing and Analysis Center® (MS-ISAC®)**, to identify what we believe to be the five most important types of attacks. We describe those attacks using the **MITRE Adversarial Tactics, Techniques, and Common Knowledge® (MITRE ATT&CK®) Framework** in order to create attack patterns (or specific combinations of Tactics and Techniques used in those attacks). This allows us to analyze the value of individual defensive actions (i.e., Safeguards[1]) against those attacks. Specifically, it also provides a consistent and explainable way to look at the security value of a given set of defensive actions across the attacker's life cycle, and provide a basis for strategies like defense-in-depth. The details of this analysis are available on the CIS website. The bottom line is that we have taken a major step towards identifying the security value of the CIS Controls, or any subset of them. While these ideas are still evolving, at CIS we are committed to the idea of security recommendations based on data, presented transparently. For additional information, reference **https://www.cisecurity.org/controls/v8/**.

These activities ensure that the CIS Security Best Practices (which include the CIS Controls and CIS Benchmarks) are more than a checklist of "good things to do," or "things that *could* help"; instead, they are a prescriptive, prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and in alignment with all industry or government security requirements.

[1] "Safeguards" were known as "Sub-Controls" prior to Version 8 of the CIS Controls.

This Version of the CIS Controls

When we begin the work of a new version, we first sit down to establish "design principles" that will be used to guide the process. These serve as a decision "touchstone" to remind us of what is really important, and of the goals of the CIS Controls. While these have been fairly consistent since the earliest versions of the CIS Controls, we have been refining our thinking over the last couple of versions to focus on the role that the CIS Controls play in the total picture of enterprise security.

Our design principles include:

- **Offense Informs Defense**
  - CIS Controls are selected, dropped, and prioritized based on data, and on specific knowledge of attacker behavior and how to stop it
- **Focus**
  - Help defenders identify the most critical things they need to do to stop the most important attacks
  - Avoid being tempted to solve every security problem—avoid adding "good things to do" or "things you could do"
- **Feasible**
  - All individual recommendations (Safeguards) must be specific and practical to implement
- **Measurable**
  - All CIS Controls, especially for Implementation Group 1, must be measurable
  - Simplify or remove ambiguous language to avoid inconsistent interpretation
  - Some Safeguards may have a threshold
- **Align**
  - Create and demonstrate "peaceful co-existence" with other governance, regulatory, process management schemes, framework, and structures
  - Cooperate with and point to existing, independent standards and security recommendations where they exist, e.g., National Institute of Standards and Technology® (NIST®), Cloud Security Alliance (CSA), Software Assurance Forum for Excellence in Code (SAFECode), ATT&CK, Open Web Application Security Project® (OWASP®)

In addition, since Version 7, we have all seen significant changes in technology and the cybersecurity ecosystem. Movement to cloud-based computing, virtualization, mobility, outsourcing, Work-from-Home, and changing attacker tactics have been central in every discussion. Physical devices, fixed boundaries, and discrete islands of security implementation are less important, and so we reflect that in Version 8, through revised terminology and grouping of Safeguards. Also, to guide adopters in implementing Version 8, CIS created a glossary to remove ambiguity of terminology. Some ideas have been combined or grouped differently to more naturally reflect the evolution of technology, rather than how enterprise teams or responsibilities might be organized, and always referring back to our guiding principles.

The text of the CIS Controls document is just one step of a process to design, implement, measure, report, and manage enterprise security. Taking this entire work stream into account as we write the CIS Controls, we can support the total enterprise management process through: making sure that each Safeguard asks for "one thing,"

wherever possible, in a way that is clear and requires minimal interpretation; that we focus on measurable actions, and define the measurement as part of the process; and, that we simplify the language to avoid duplication.

At CIS, we have always tried to be very conscious of the balance between addressing current topics and the stability of an overall defensive improvement program. We have always tried to focus on the foundations of good cyber defense—and, always tried to keep our eyes on emerging new defensive technology—while avoiding the "shiny new toys" or complex technology that is out of reach for most enterprises.

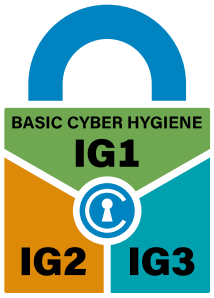
The CIS Controls Ecosystem ("It's not about the list")

Whether you use the CIS Controls, and/or another way to guide your security improvement program, you should recognize that "it's not about the list." You can get a credible list of security recommendations from many sources—it is best to think of the list as a starting point. It is important to look for the ecosystem that grows up around the list. Where can I get training, complementary information, explanations; how have others implemented and used these recommendations; is there a marketplace of vendor tools and services to choose from; how will I measure progress or maturity; how does this align with the myriad regulatory and compliance frameworks that apply to me? The true power of the CIS Controls is not about creating the best list, it is about harnessing the experience of a community of individuals and enterprises to actually make security improvements through the sharing of ideas, tools, lessons, and collective action.

To support this, CIS acts as a catalyst and clearinghouse to help us all learn from each other. Since Version 6, there has been an explosion of complementary information, products, and services available from CIS, and from the industry-at-large. Please contact CIS for the following kinds of working aids and other support materials, https://www.cisecurity.org/controls/v8/:

- Mappings from the CIS Controls to a very wide variety for formal Risk Management Frameworks (like NIST®, Federal Information Security Modernization Act (FISMA), International Organization for Standardization (ISO), etc.)
- Use cases of enterprise adoption
- A list of ongoing references to the CIS Controls in national and international standards, state and national legislation and regulation, trade and professional associations, etc.
- Information tailored for small and medium enterprises
- Measurement and metrics for the CIS Controls
- Pointers to vendor white papers and other materials that support the CIS Controls
- Documentation on alignment with the NIST® Cybersecurity Framework

How to Get Started



Historically, the CIS Controls were ordered in sequence to focus an enterprise's cybersecurity activities, with a subset of the first six CIS Controls referred to as "cyber hygiene." However, this proved to be too simplistic. Enterprises, especially small ones, could struggle with some of the early Safeguards and never get around to implementing later CIS Controls (for example, having a backup strategy to help recover from ransomware). As a result, starting with Version 7.1, we created CIS Controls Implementation Groups (IGs) as our recommended new guidance to prioritize implementation.

The CIS Controls IGs are self-assessed categories for enterprises. Each IG identifies a subset of the CIS Controls that the community has broadly assessed to be applicable for an enterprise with a similar risk profile and resources to strive to implement. These IGs represent a horizontal look across the CIS Controls tailored to different types of enterprises. Specifically, we have defined IG1 as "basic cyber hygiene," the foundational set of cyber defense Safeguards that every enterprise should apply to guard against the most common attacks (https://www.cisecurity.org/controls/v8/). Each IG then builds upon the previous one: IG2 includes IG1, and IG3 includes all CIS Safeguards in IG1 and IG2.

Using or Transitioning from Prior Versions of the CIS Controls

We believe that Version 8 of the CIS Controls is the best we have ever produced. We also appreciate that enterprises who are actively using prior versions of the CIS Controls as a key part of their defensive strategy might be reluctant to move to Version 8. Our recommendation is that if you are using Version 7 or Version 7.1, you are following an effective and usable security plan, and over time you should consider moving to Version 8. If you are using Version 6 (or earlier), our recommendation is that you should start to plan a transition to Version 8 as soon as practicable.

For prior versions of the CIS Controls, we were able to provide only the simplest tools to aid in transition from prior versions, basically a spreadsheet-based change log. For Version 8, we have taken a much more holistic approach and worked with numerous partners to ensure that the CIS Controls ecosystem is ready to support your transition, https://www.cisecurity.org/controls/v8/.

Structure of the CIS Controls

The presentation of each Control in this document includes the following elements:

- **Overview.** A brief description of the intent of the Control and its utility as a defensive action
- **Why is this Control critical?** A description of the importance of this Control in blocking, mitigating, or identifying attacks, and an explanation of how attackers actively exploit the absence of this Control
- **Procedures and tools.** A more technical description of the processes and technologies that enable implementation and automation of this Control
- **Safeguard descriptions.** A table of the specific actions that enterprises should take to implement the Control

Implementation Groups

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 (Includes IG1)

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 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 (Includes IG1 and IG2)

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.

CIS Controls

CONTROL 01

Inventory and Control of Enterprise Assets

Safeguards Total	5	IG1	2/5	IG2	4/5	IG3	5/5

Overview

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.

Why is this Control critical?

Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them, and proper asset management will help identify those enterprise assets that hold or manage this critical data, so that appropriate security controls can be applied.

External attackers are continuously scanning the internet address space of target enterprises, premise-based or in the cloud, identifying possibly unprotected assets attached to an enterprise's network. Attackers can take advantage of new assets that are installed, yet not securely configured and patched. Internally, unidentified assets can also have weak security configurations that can make them vulnerable to web- or email-based malware; and, adversaries can leverage weak security configurations for traversing the network, once they are inside.

Additional assets that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks) should be identified and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

Large, complex, dynamic enterprises understandably struggle with the challenge of managing intricate, fast-changing environments. However, attackers have shown the ability, patience, and willingness to "inventory and control" our enterprise assets at very large scale in order to support their opportunities.

Another challenge is that portable end-user devices will periodically join a network and then disappear, making the inventory of currently available assets very dynamic. Likewise, cloud environments and virtual machines can be difficult to track in asset inventories when they are shut down or paused.

Another benefit of complete enterprise asset management is supporting incident response, both when investigating the origination of network traffic from an asset on the network and when identifying all potentially vulnerable, or impacted, assets of similar type or location during an incident.

Procedures and tools

This CIS Control requires both technical and procedural actions, united in a process that accounts for, and manages the inventory of, enterprise assets and all associated data throughout its life cycle. It also links to business governance through establishing data/asset owners who are responsible for each component of a business process. Enterprises can use large-scale, comprehensive enterprise products to maintain IT asset inventories. Smaller enterprises can leverage security tools already installed on enterprise assets or used on the network to collect this data. This includes doing a discovery scan of the network with a vulnerability scanner; reviewing anti-malware logs, logs from endpoint security portals, network logs from switches, or authentication logs; and managing the results in a spreadsheet or database.

Maintaining a current and accurate view of enterprise assets is an ongoing and dynamic process. Even for enterprises, there is rarely a single source of truth, as enterprise assets are not always provisioned or installed by the IT department. The reality is that a variety of sources need to be "crowd-sourced" to determine a high-confidence count of enterprise assets. Enterprises can actively scan on a regular basis, sending a variety of different packet types to identify assets connected to the network. In addition to asset sources mentioned above for small enterprises, larger enterprises can collect data from cloud portals and logs from enterprise platforms such as: Active Directory (AD), Single Sign-On (SSO), Multi-Factor Authentication (MFA), Virtual Private Network (VPN), Intrusion Detection Systems (IDS) or Deep Packet Inspection (DPI), Mobile Device Management (MDM), and vulnerability scanning tools. Property inventory databases, purchase order tracking, and local inventory lists are other sources of data to determine which devices are connected. There are tools and methods that normalize this data to identify devices that are unique among these sources.

→ **For cloud-specific guidance, refer to the CIS Controls Cloud Companion Guide –** https://www.cisecurity.org/controls/v8/

→ **For tablet and smart phone guidance, refer to the CIS Controls Mobile Companion Guide –** https://www.cisecurity.org/controls/v8/

→ **For IoT guidance, refer to the CIS Controls Internet of Things Companion Guide –** https://www.cisecurity.org/controls/v8/

→ **For Industrial Control Systems (ICS) guidance, refer to the CIS Controls ICS Implementation Guide –** https://www.cisecurity.org/controls/v8/

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
1.1	**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, data 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.	Devices	Identify	●	●	●
1.2	**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.	Devices	Respond	●	●	●
1.3	**Utilize an Active Discovery Tool** Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.	Devices	Detect		●	●
1.4	**Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory** Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.	Devices	Identify		●	●
1.5	**Use a Passive Asset Discovery Tool** Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.	Devices	Detect			●

CONTROL 02

Inventory and Control of Software Assets

Safeguards Total 7 | IG1 3/7 | IG2 6/7 | IG3 7/7

Overview

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

Why is this Control critical?

A complete software inventory is a critical foundation for preventing attacks. Attackers continuously scan target enterprises looking for vulnerable versions of software that can be remotely exploited. For example, if a user opens a malicious website or attachment with a vulnerable browser, an attacker can often install backdoor programs and bots that give the attacker long-term control of the system. Attackers can also use this access to move laterally through the network. One of the key defenses against these attacks is updating and patching software. However, without a complete inventory of software assets, an enterprise cannot determine if they have vulnerable software, or if there are potential licensing violations.

Even if a patch is not yet available, a complete software inventory list allows an enterprise to guard against known attacks until the patch is released. Some sophisticated attackers use "zero-day exploits," which take advantage of previously unknown vulnerabilities that have yet to have a patch released from the software vendor. Depending on the severity of the exploit, an enterprise can implement temporary mitigation measures to guard against attacks until the patch is released.

Management of software assets is also important to identify unnecessary security risks. An enterprise should review its software inventory to identify any enterprise assets running software that is not needed for business purposes. For example, an enterprise asset may come installed with default software that creates a potential security risk and provides no benefit to the enterprise. It is critical to inventory, understand, assess, and manage all software connected to an enterprise's infrastructure.

Procedures and tools

Allowlisting can be implemented using a combination of commercial allowlisting tools, policies, or application execution tools that come with anti-malware suites and popular operating systems. Commercial software inventory tools are widely available and used in many enterprises today. The best of these tools provides an inventory check of hundreds of common software used in enterprises. The tools pull information about the patch level of each installed program to ensure that it is the latest version and leverage standardized application names, such as those found in the Common Platform Enumeration (CPE) specification. One example of a method that can be used is the Security Content Automation Protocol (SCAP). Additional information on SCAP can be found here: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

Features that implement allowlists are included in many modern endpoint security suites and even natively implemented in certain versions of major operating systems. Moreover, commercial solutions are increasingly bundling together anti-malware, anti-spyware, personal firewall, and host-based IDS and Intrusion Prevention System (IPS), along with application allow and block listing. In particular, most endpoint security solutions can look at the name, file system location, and/or cryptographic hash of a given executable to determine whether the application should be allowed to run on the protected machine. The most effective of these tools offer custom allowlists based on executable path, hash, or regular expression matching. Some even include a non-malicious, yet unapproved, applications function that allows administrators to define rules for execution of specific software for certain users and at certain times of the day.

→ **For cloud-specific guidance, refer to the CIS Controls Cloud Companion Guide –** https://www.cisecurity.org/controls/v8/

→ **For tablet and smart phone guidance, refer to the CIS Controls Mobile Companion Guide –** https://www.cisecurity.org/controls/v8/

→ **For IoT guidance, refer to the CIS Controls Internet of Things Companion Guide –** https://www.cisecurity.org/controls/v8/

→ **For Industrial Control Systems (ICS) guidance, refer to the CIS Controls ICS Implementation Guide –** https://www.cisecurity.org/controls/v8/

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
2.1	**Establish and Maintain a Software Inventory** Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Applications	Identify	●	●	●
2.2	**Ensure Authorized Software is Currently Supported** Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Applications	Identify	●	●	●

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
2.3	**Address Unauthorized Software** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Applications	Respond	●	●	●
2.4	**Utilize Automated Software Inventory Tools** Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.	Applications	Detect		●	●
2.5	**Allowlist Authorized Software** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	Applications	Protect		●	●
2.6	**Allowlist Authorized Libraries** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.	Applications	Protect		●	●
2.7	**Allowlist Authorized Scripts** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.	Applications	Protect			●

CONTROL 03

Data Protection

Safeguards Total 14 — IG1 6/14 — IG2 12/14 — IG3 14/14

Overview

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Why is this Control critical?

Data is no longer only contained within an enterprise's border; it is in the cloud, on portable end-user devices where users work from home, and is often shared with partners or online services that might have it anywhere in the world. In addition to sensitive data an enterprise holds related to finances, intellectual property, and customer data, there also might be numerous international regulations for protection of personal data. Data privacy has become increasingly important, and enterprises are learning that privacy is about the appropriate use and management of data, not just encryption. Data must be appropriately managed through its entire life cycle. These privacy rules can be complicated for multi-national enterprises of any size; however, there are fundamentals that can apply to all.

Once attackers have penetrated an enterprise's infrastructure, one of their first tasks is to find and exfiltrate data. Enterprises might not be aware that sensitive data is leaving their environment because they are not monitoring data outflows.

While many attacks occur on the network, others involve physical theft of portable end-user devices, attacks on service providers or other partners holding sensitive data. Other sensitive enterprise assets may also include non-computing devices that provide management and control of physical systems, such as Supervisory Control and Data Acquisition (SCADA) systems.

The enterprise's loss of control over protected or sensitive data is a serious and often reportable business impact. While some data is compromised or lost as a result of theft or espionage, the vast majority are a result of poorly understood data management rules, and user error. The adoption of data encryption, both in transit and at rest, can provide mitigation against data compromise, and, even more important, it is a regulatory requirement for most controlled data.

Procedures and tools

It is important for an enterprise to develop a data management process that includes a data management framework, data classification guidelines, and requirements for protection, handling, retention, and disposal of data. There should also be a data breach process that plugs into the incident response plan, and the compliance and communication plans. To derive data sensitivity levels, enterprises need to catalog their key types of data and the overall criticality (impact to its loss or corruption) to the enterprise. This analysis would be used to create an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels.

Once the sensitivity of the data has been defined, a data inventory or mapping should be developed that identifies software accessing data at various sensitivity levels and the enterprise assets that house those applications. Ideally, the network would be separated so that enterprise assets of the same sensitivity level are on the same network and separated from enterprise assets with different sensitivity levels. If possible, firewalls need to control access to each segment, and have user access rules applied to only allow those with a business need to access the data.

For more comprehensive treatment of this topic, we suggest the following resources to help the enterprise with data protection:

- **NIST® SP 800-88r1 Guides for Media Sanitization –** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
- **NIST® FIPS 140-2 –** https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
- **NIST® FIPS 140-3 –** https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
- **For cloud-specific guidance, refer to the CIS Controls Cloud Companion Guide –** https://www.cisecurity.org/controls/v8/
- **For tablet and smart phone guidance, refer to the CIS Controls Mobile Companion Guide –** https://www.cisecurity.org/controls/v8/

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
3.1	**Establish and Maintain a Data Management Process** Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify	●	●	●
3.2	**Establish and Maintain a Data Inventory** Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	Data	Identify	●	●	●
3.3	**Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Data	Protect	●	●	●

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
3.4	**Enforce Data Retention** Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	Data	Protect	●	●	●
3.5	**Securely Dispose of Data** Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	Data	Protect	●	●	●
3.6	**Encrypt Data on End-User Devices** Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Devices	Protect	●	●	●
3.7	**Establish and Maintain a Data Classification Scheme** Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify		●	●
3.8	**Document Data Flows** Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify		●	●
3.9	**Encrypt Data on Removable Media** Encrypt data on removable media.	Data	Protect		●	●
3.10	**Encrypt Sensitive Data in Transit** Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).	Data	Protect		●	●
3.11	**Encrypt Sensitive Data at Rest** Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.	Data	Protect		●	●
3.12	**Segment Data Processing and Storage Based on Sensitivity** Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.	Network	Protect		●	●
3.13	**Deploy a Data Loss Prevention Solution** Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.	Data	Protect			●
3.14	**Log Sensitive Data Access** Log sensitive data access, including modification and disposal.	Data	Detect			●

CONTROL 04

Secure Configuration of Enterprise Assets and Software

Safeguards Total 12 | IG1 7/12 | IG2 11/12 | IG3 12/12

Overview

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Why is this Control critical?

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

Service providers play a key role in modern infrastructures, especially for smaller enterprises. They often are not set up by default in the most secure configuration to provide flexibility for their customers to apply their own security policies. Therefore, the presence of default accounts or passwords, excessive access, or unnecessary services are common in default configurations. These could introduce weaknesses that are under the responsibility of the enterprise that is using the software, rather than the service provider. This extends to ongoing management and updates, as some Platform as a Service (PaaS) only extend to the operating system, so patching and updating hosted applications are under the responsibility of the enterprise.

Even after a strong initial configuration is developed and applied, it must be continually managed to avoid degrading security as software is updated or patched, new security vulnerabilities are reported, and configurations are "tweaked," to allow the installation of new software or to support new operational requirements.

Procedures and tools

There are many available security baselines for each system. Enterprises should start with these publicly developed, vetted, and supported security benchmarks, security guides, or checklists. Some resources include:

- **The CIS Benchmarks™ Program – http://www.cisecurity.org/cis-benchmarks/**
- **The National Institute of Standards and Technology (NIST®) National Checklist Program Repository – https://nvd.nist.gov/ncp/repository**

Enterprises should augment or adjust these baselines to satisfy enterprise security policies, and industry and government regulatory requirements. Deviations of standard configurations and rationale should be documented to facilitate future reviews or audits.

For a larger or more complex enterprise, there will be multiple security baseline configurations based on security requirements or classification of the data on the enterprise asset. Here is an example of the steps to build a secure baseline image:

01 Determine the risk classification of the data handled/stored on the enterprise asset (e.g., high, moderate, low risk).

02 Create a security configuration script that sets system security settings to meet the requirements to protect the data used on the enterprise asset. Use benchmarks, such as the ones described earlier in this section.

03 Install the base operating system software.

04 Apply appropriate operating system and security patches.

05 Install appropriate application software packages, tool, and utilities.

06 Apply appropriate updates to software installed in Step 4.

07 Install local customization scripts to this image.

08 Run the security script created in Step 2 to set the appropriate security level.

09 Run a SCAP compliant tool to record/score the system setting of the baseline image.

10 Perform a security quality assurance test.

11 Save this base image in a secure location.

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

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
4.1	**Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/IoT devices; and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect	●	●	●
4.2	**Establish and Maintain a Secure Configuration Process for Network Infrastructure** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Network	Protect	●	●	●
4.3	**Configure Automatic Session Locking on Enterprise Assets** Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	Users	Protect	●	●	●
4.4	**Implement and Manage a Firewall on Servers** Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	Devices	Protect	●	●	●
4.5	**Implement and Manage a Firewall on End-User Devices** Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Devices	Protect	●	●	●
4.6	**Securely Manage Enterprise Assets and Software** Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	Network	Protect	●	●	●
4.7	**Manage Default Accounts on Enterprise Assets and Software** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	Users	Protect	●	●	●
4.8	**Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.	Devices	Protect		●	●
4.9	**Configure Trusted DNS Servers on Enterprise Assets** Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.	Devices	Protect		●	●
4.10	**Enforce Automatic Device Lockout on Portable End-User Devices** Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.	Devices	Respond		●	●
4.11	**Enforce Remote Wipe Capability on Portable End-User Devices** Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.	Devices	Protect		●	●
4.12	**Separate Enterprise Workspaces on Mobile End-User Devices** Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.	Devices	Protect			●

CONTROL 05

Account Management

Safeguards Total	6	IG1	4/6	IG2	6/6	IG3	6/6

Overview

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Why is this Control critical?

It is easier for an external or internal threat actor to gain unauthorized access to enterprise assets or data through using valid user credentials than through "hacking" the environment. There are many ways to covertly obtain access to user accounts, including: weak passwords, accounts still valid after a user leaves the enterprise, dormant or lingering test accounts, shared accounts that have not been changed in months or years, service accounts embedded in applications for scripts, a user having the same password as one they use for an online account that has been compromised (in a public password dump), social engineering a user to give their password, or using malware to capture passwords or tokens in memory or over the network.

Administrative, or highly privileged, accounts are a particular target, because they allow attackers to add other accounts, or make changes to assets that could make them more vulnerable to other attacks. Service accounts are also sensitive, as they are often shared among teams, internal and external to the enterprise, and sometimes not known about, only to be revealed in standard account management audits.

Finally, account logging and monitoring is a critical component of security operations. While account logging and monitoring are covered in CIS Control 8 (Audit Log Management), it is important in the development of a comprehensive Identity and Access Management (IAM) program.

Procedures and tools

Credentials are assets that must be inventoried and tracked like enterprise assets and software, as they are the primary entry point into the enterprise. Appropriate password policies and guidance not to reuse passwords should be developed.

→ **For guidance on the creation and use of passwords, reference the CIS Password Policy Guide –** https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Accounts must also be tracked; any account that is dormant must be disabled and eventually removed from the system. There should be periodic audits to ensure all active accounts are traced back to authorized users of the enterprise asset. Look for new accounts added since previous review, especially administrator and service accounts. Close attention should be made to identify and track administrative, or high-privileged accounts and service accounts.

Users with administrator or other privileged access should have separate accounts for those higher authority tasks. These accounts would only be used when performing those tasks or accessing especially sensitive data, to reduce risk in case their normal user account is compromised. For users with multiple accounts, their base user account, used day-to-day for non-administrative tasks, should not have any elevated privileges.

Single Sign-On (SSO) is convenient and secure when an enterprise has many applications, including cloud applications, which helps reduce the number of passwords a user must manage. Users are recommended to use password manager applications to securely store their passwords, and should be instructed not to keep them in spreadsheets or text files on their computers. MFA is recommended for remote access.

Users must also be automatically logged out of the system after a period of inactivity, and be trained to lock their screen when they leave their device to minimize the possibility of someone else in physical proximity around the user accessing their system, applications, or data.

→ **An excellent resource is the NIST® Digital Identity Guidelines –** https://pages.nist.gov/800-63-3/

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
5.1	**Establish and Maintain an Inventory of Accounts** Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Users	Identify	●	●	●
5.2	**Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	Users	Protect	●	●	●

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
5.3	**Disable Dormant Accounts** Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	Users	Respond	●	●	●
5.4	**Restrict Administrator Privileges to Dedicated Administrator Accounts** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	Users	Protect	●	●	●
5.5	**Establish and Maintain an Inventory of Service Accounts** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Users	Identify		●	●
5.6	**Centralize Account Management** Centralize account management through a directory or identity service.	Users	Protect		●	●

CONTROL 06

Access Control Management

Safeguards Total	8	IG1	5/8	IG2	7/8	IG3	8/8

Overview

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Why is this Control critical?

Where CIS Control 5 deals specifically with account management, CIS Control 6 focuses on managing what access these accounts have, ensuring users only have access to the data or enterprise assets appropriate for their role, and ensuring that there is strong authentication for critical or sensitive enterprise data or functions. Accounts should only have the minimal authorization needed for the role. Developing consistent access rights for each role and assigning roles to users is a best practice. Developing a program for complete provision and de-provisioning access is also important. Centralizing this function is ideal.

There are some user activities that pose greater risk to an enterprise, either because they are accessed from untrusted networks, or performing administrator functions that allow the ability to add, change, or remove other accounts, or make configuration changes to operating systems or applications to make them less secure. This also enforces the importance of using MFA and Privileged Access Management (PAM) tools.

Some users have access to enterprise assets or data they do not need for their role; this might be due to an immature process that gives all users all access, or lingering access as users change roles within the enterprise over time. Local administrator privileges to users' laptops is also an issue, as any malicious code installed or downloaded by the user can have greater impact on the enterprise asset running as administrator. User, administrator, and service account access should be based on enterprise role and need.

Procedures and tools

There should be a process where privileges are granted and revoked for user accounts. This ideally is based on enterprise role and need through role-based access. Role-based access is a technique to define and manage access requirements for each account based on: need to know, least privilege, privacy requirements, and/or separation of duties. There are technology tools to help manage this process. However, there might be more granular or temporary access based on circumstance.

MFA should be universal for all privileged or administrator accounts. There are many tools that have smartphone applications to perform this function, and are easy to deploy. Using the number-generator feature is more secure than just sending a Short Messaging Service (SMS) message with a one-time code, or prompting a "push" alert for a user to accept. However, neither is recommended for privileged account MFA. PAM tools are available for privileged account control, and provide a one-time password that must be checked out for each use. For additional security in system administration, using "jump-boxes" or out of band terminal connections is recommended.

Comprehensive account de-provisioning is important. Many enterprises have repeatable consistent processes for removing access when employees leave the enterprise. However, that process is not always consistent for contractors, and must be included in the standard de-provisioning process. Enterprises should also inventory and track service accounts, as a common error is leaving clear text tokens or passwords in code, and posting to public cloud-based code repositories.

High-privileged accounts should not be used for day-to-day use, such as web surfing and email reading. Administrators should have separate accounts that do not have elevated privileges for daily office use, and should log into administrator accounts only when performing administrator functions requiring that level of authorization. Security personnel should periodically gather a list of running processes to determine whether any browsers or email readers are running with high privileges.

→ **An excellent resource is the NIST® Digital Identity Guidelines –** https://pages.nist.gov/800-63-3/

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
6.1	**Establish an Access Granting Process** Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	Users	Protect	●	●	●
6.2	**Establish an Access Revoking Process** Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	Users	Protect	●	●	●
6.3	**Require MFA for Externally-Exposed Applications** Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	Users	Protect	●	●	●

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
6.4	**Require MFA for Remote Network Access** Require MFA for remote network access.	Users	Protect	●	●	●
6.5	**Require MFA for Administrative Access** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	Users	Protect	●	●	●
6.6	**Establish and Maintain an Inventory of Authentication and Authorization Systems** Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.	Users	Identify		●	●
6.7	**Centralize Access Control** Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.	Users	Protect		●	●
6.8	**Define and Maintain Role-Based Access Control** Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.	Data	Protect			●

CONTROL 07

Continuous Vulnerability Management

Safeguards Total	7	IG1	4/7	IG2	7/7	IG3	7/7

Overview

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Why is this Control critical?

Cyber defenders are constantly being challenged from attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Defenders must have timely threat information available to them about: software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

Attackers have access to the same information and can often take advantage of vulnerabilities more quickly than an enterprise can remediate. While there is a gap in time from a vulnerability being known to when it is patched, defenders can prioritize which vulnerabilities are most impactful to the enterprise, or likely to be exploited first due to ease of use. For example, when researchers or the community report new vulnerabilities, vendors have to develop and deploy patches, indicators of compromise (IOCs), and updates. Defenders need to assess the risk of the new vulnerability to the enterprise, regression-test patches, and install the patch.

There is never perfection in this process. Attackers might be using an exploit to a vulnerability that is not known within the security community. They might have developed an exploit to this vulnerability referred to as a "zero-day" exploit. Once the vulnerability is known in the community, the process mentioned above starts. Therefore, defenders must keep in mind that an exploit might already exist when the vulnerability is widely socialized. Sometimes vulnerabilities might be known within a closed community (e.g., vendor still developing a fix) for weeks, months, or years before it is disclosed publicly. Defenders have to be aware that there might always be vulnerabilities they cannot remediate, and therefore need to use other controls to mitigate.

Enterprises that do not assess their infrastructure for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their enterprise assets compromised. Defenders face particular challenges in scaling remediation across an entire enterprise, and prioritizing actions with conflicting priorities, while not impacting the enterprise's business or mission.

Procedures and tools

A large number of vulnerability scanning tools are available to evaluate the security configuration of enterprise assets. Some enterprises have also found commercial services using remotely managed scanning appliances to be effective. To help standardize the definitions of discovered vulnerabilities across an enterprise, it is preferable to use vulnerability scanning tools that map vulnerabilities to one or more of the following industry-recognized vulnerability, configuration and platform classification schemes and languages: Common Vulnerabilities and Exposures (CVE®), Common Configuration Enumeration (CCE), Open Vulnerability and Assessment Language (OVAL®), Common Platform Enumeration (CPE), Common Vulnerability Scoring System (CVSS), and/or Extensible Configuration Checklist Description Format (XCCDF). These schemes and languages are components of SCAP.

→ **More information on SCAP can be found here – https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf**

The frequency of scanning activities should increase as the diversity of an enterprise's assets increases to account for the varying patch cycles of each vendor. Advanced vulnerability scanning tools can be configured with user credentials to authenticate into enterprise assets and perform more comprehensive assessments. These are called "authenticated scans."

In addition to the scanning tools that check for vulnerabilities and misconfigurations across the network, various free and commercial tools can evaluate security settings and configurations of enterprise assets. Such tools can provide fine-grained insight into unauthorized changes in configuration or the inadvertent introduction of security weaknesses from administrators.

Effective enterprises link their vulnerability scanners with problem-ticketing systems that track and report progress on fixing vulnerabilities. This can help highlight unmitigated critical vulnerabilities to senior management to ensure they are resolved. Enterprises can also track how long it took to remediate a vulnerability, after identified, or a patch has been issued. These can support internal or industry compliance requirements. Some mature enterprises will go over these reports in IT security steering committee meetings, which bring leaders from IT and the business together to prioritize remediation efforts based on business impact.

In selecting which vulnerabilities to fix, or patches to apply, an enterprise should augment NIST's Common Vulnerability Scoring System (CVSS) with data concerning the likelihood of a threat actor using a vulnerability, or potential impact of an exploit to the enterprise. Information on the likelihood of exploitation should also be periodically updated based on the most current threat information. For example, the release of a new exploit, or new intelligence relating to exploitation of the vulnerability, should change the priority through which the vulnerability should be considered for patching. Various commercial systems are available to allow an enterprise to automate and maintain this process in a scalable manner.

The most effective vulnerability scanning tools compare the results of the current scan with previous scans to determine how the vulnerabilities in the environment have changed over time. Security personnel use these features to conduct vulnerability trending from month to month.

Finally, there should be a quality assurance process to verify configuration updates, or that patches are implemented correctly and across all relevant enterprise assets.

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
7.1	**Establish and Maintain a Vulnerability Management Process** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect	●	●	●
7.2	**Establish and Maintain a Remediation Process** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	Applications	Respond	●	●	●
7.3	**Perform Automated Operating System Patch Management** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Applications	Protect	●	●	●
7.4	**Perform Automated Application Patch Management** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Applications	Protect	●	●	●
7.5	**Perform Automated Vulnerability Scans of Internal Enterprise Assets** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.	Applications	Identify		●	●
7.6	**Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.	Applications	Identify		●	●
7.7	**Remediate Detected Vulnerabilities** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.	Applications	Respond		●	●

CONTROL 08

Audit Log Management

Safeguards Total 12 — IG1 3/12 — IG2 11/12 — IG3 12/12

Overview

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Why is this Control critical?

Log collection and analysis is critical for an enterprise's ability to detect malicious activity quickly. Sometimes audit records are the only evidence of a successful attack. Attackers know that many enterprises keep audit logs for compliance purposes, but rarely analyze them. Attackers use this knowledge to hide their location, malicious software, and activities on victim machines. Due to poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target enterprise knowing.

There are two types of logs that are generally treated and often configured independently: system logs and audit logs. System logs typically provide system-level events that show various system process start/end times, crashes, etc. These are native to systems, and take less configuration to turn on. Audit logs typically include user-level events—when a user logged in, accessed a file, etc.—and take more planning and effort to set up.

Logging records are also critical for incident response. After an attack has been detected, log analysis can help enterprises understand the extent of an attack. Complete logging records can show, for example, when and how the attack occurred, what information was accessed, and if data was exfiltrated. Retention of logs is also critical in case a follow-up investigation is required or if an attack remained undetected for a long period of time.

Procedures and tools

Most enterprise assets and software offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (Virtual Private Network (VPN), dial-up, etc.) should all be configured for verbose logging where beneficial. Retention of logging data is also important in the event an incident investigation is required.

Furthermore, all enterprise assets should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, an enterprise should periodically scan through its logs and compare them with the enterprise asset inventory assembled as part of CIS Control 1, in order to ensure that each managed asset actively connected to the network is periodically generating logs.

Safeguards

NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
8.1	**Establish and Maintain an Audit Log Management Process** Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Network	Protect	●	●	●
8.2	**Collect Audit Logs** Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	Network	Detect	●	●	●
8.3	**Ensure Adequate Audit Log Storage** Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	Network	Protect	●	●	●
8.4	**Standardize Time Synchronization** Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.	Network	Protect		●	●
8.5	**Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.	Network	Detect		●	●
8.6	**Collect DNS Query Audit Logs** Collect DNS query audit logs on enterprise assets, where appropriate and supported.	Network	Detect		●	●
8.7	**Collect URL Request Audit Logs** Collect URL request audit logs on enterprise assets, where appropriate and supported.	Network	Detect		●	●
8.8	**Collect Command-Line Audit Logs** Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.	Devices	Detect		●	●
8.9	**Centralize Audit Logs** Centralize, to the extent possible, audit log collection and retention across enterprise assets.	Network	Detect		●	●
8.10	**Retain Audit Logs** Retain audit logs across enterprise assets for a minimum of 90 days.	Network	Protect		●	●
8.11	**Conduct Audit Log Reviews** Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.	Network	Detect		●	●
8.12	**Collect Service Provider Logs** Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.	Data	Detect			●

CONTROL 09

Email and Web Browser Protections

Safeguards Total 7 | IG1 2/7 | IG2 6/7 | IG3 7/7

Overview

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Why is this Control critical?

Web browsers and email clients are very common points of entry for attackers because of their direct interaction with users inside an enterprise. Content can be crafted to entice or spoof users into disclosing credentials, providing sensitive data, or providing an open channel to allow attackers to gain access, thus increasing risk to the enterprise. Since email and web are the main means that users interact with external and untrusted users and environments, these are prime targets for both malicious code and social engineering. Additionally, as enterprises move to web-based email, or mobile email access, users no longer use traditional full-featured email clients, which provide embedded security controls like connection encryption, strong authentication, and phishing reporting buttons.

Procedures and tools

Web Browser

Cybercriminals can exploit web browsers in multiple ways. If they have access to exploits of vulnerable browsers, they can craft malicious webpages that can exploit those vulnerabilities when browsed with an insecure, or unpatched, browser. Alternatively, they can try to target any number of common web browser third-party plugins that may allow them to hook into the browser or even directly into the operating system or application. These plugins, much like any other software within an environment, need to be reviewed for vulnerabilities, kept up-to-date with latest patches or versions, and controlled. Many come from untrusted sources, and some are even written to be malicious. Therefore, it is best to prevent users from intentionally or unintentionally installing malware that might be hiding in some of these plugins, extensions, and add-ons. Simple configuration updates to the browser can make it much harder for malware to get installed through reducing the ability of installing add-ons/plugins/extensions and preventing specific types of content from automatically executing.

Most popular browsers employ a database of phishing and/or malware sites to protect against the most common threats. A best practice is to enable these content filters and turn on the pop-up blockers. Pop-ups are not only annoying; they can also host embedded malware directly or lure users into clicking links using social engineering tricks. To help enforce blocking of known malicious domains, also consider subscribing to DNS filtering services to block attempts to access these websites at the network level.

Email

Email represents one the most interactive ways humans work with enterprise assets; training and encouraging the right behavior is just as important as the technical settings. Email is the most common threat vector against enterprises through tactics such as phishing and Business Email Compromise (BEC).

Using a spam-filtering tool and malware scanning at the email gateway reduces the number of malicious emails and attachments that come into the enterprise's network. Initiating Domain-based Message Authentication, Reporting, and Conformance (DMARC) helps reduce spam and phishing activities. Installing an encryption tool to secure email and communications adds another layer of user and network-based security. In addition to blocking based on the sender, it is also worthwhile to only allow certain file types that users need for their jobs. This will require coordination with different business units to understand what types of files they receive via email to ensure that there is not an interruption to their processes.

Since phishing email techniques are ever evolving to get past Something Posing as Mail (SPAM) filter rules, it is important to train users on how to identify phishing, and to notify IT Security when they see one. There are many platforms that perform phishing tests against users to help educate them on different examples, and track their improvement over time. Crowd-sourcing this knowledge into notifying IT Security teams of phishing helps improve the protections and detections of email-based threats.

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
9.1	**Ensure Use of Only Fully Supported Browsers and Email Clients** Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	Applications	Protect	●	●	●
9.2	**Use DNS Filtering Services** Use DNS filtering services on all enterprise assets to block access to known malicious domains.	Network	Protect	●	●	●
9.3	**Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.	Network	Protect		●	●
9.4	**Restrict Unnecessary or Unauthorized Browser and Email Client Extensions** Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.	Applications	Protect		●	●

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
9.5	**Implement DMARC** To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.	Network	Protect		●	●
9.6	**Block Unnecessary File Types** Block unnecessary file types attempting to enter the enterprise's email gateway.	Network	Protect		●	●
9.7	**Deploy and Maintain Email Server Anti-Malware Protections** Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.	Network	Protect			●

CONTROL 10

Malware Defenses

Safeguards Total	7	IG1	3/7	IG2	7/7	IG3	7/7

Overview

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Why is this Control critical?

Malicious software (sometimes categorized as viruses or Trojans) is an integral and dangerous aspect of internet threats. They can have many purposes, from capturing credentials, stealing data, identifying other targets within the network, and encrypting or destroying data. Malware is ever-evolving and adaptive, as modern variants leverage machine learning techniques.

Malware enters an enterprise through vulnerabilities within the enterprise on end-user devices, email attachments, webpages, cloud services, mobile devices, and removable media. Malware often relies on insecure end-user behavior, such as clicking links, opening attachments, installing software or profiles, or inserting Universal Serial Bus (USB) flash drives. Modern malware is designed to avoid, deceive, or disable defenses.

Malware defenses must be able to operate in this dynamic environment through automation, timely and rapid updating, and integration with other processes like vulnerability management and incident response. They must be deployed at all possible entry points and enterprise assets to detect, prevent spread, or control the execution of malicious software or code.

Procedures and tools

Effective malware protection includes traditional endpoint malware prevention and detection suites. To ensure malware IOCs are up-to-date, enterprises can receive automated updates from the vendor to enrich other vulnerability or threat data. These tools are best managed centrally to provide consistency across the infrastructure.

Being able to block or identify malware is only part of this CIS Control; there is also a focus on centrally collecting the logs to support alerting, identification, and incident response. As malicious actors continue to develop their methodologies, many are starting to take a "living-off-the-land" (LotL) approach to minimize the likelihood of being caught. This approach refers to attacker behavior that uses tools or features that already exist in the target environment. Enabling logging, as per the Safeguards in CIS Control 8, will make it significantly easier for the enterprise to follow the events to understand what happened and why it happened.

Safeguards

NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
10.1	**Deploy and Maintain Anti-Malware Software** Deploy and maintain anti-malware software on all enterprise assets.	Devices	Protect	●	●	●
10.2	**Configure Automatic Anti-Malware Signature Updates** Configure automatic updates for anti-malware signature files on all enterprise assets.	Devices	Protect	●	●	●
10.3	**Disable Autorun and Autoplay for Removable Media** Disable autorun and autoplay auto-execute functionality for removable media.	Devices	Protect	●	●	●
10.4	**Configure Automatic Anti-Malware Scanning of Removable Media** Configure anti-malware software to automatically scan removable media.	Devices	Detect		●	●
10.5	**Enable Anti-Exploitation Features** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.	Devices	Protect		●	●
10.6	**Centrally Manage Anti-Malware Software** Centrally manage anti-malware software.	Devices	Protect		●	●
10.7	**Use Behavior-Based Anti-Malware Software** Use behavior-based anti-malware software.	Devices	Detect		●	●

CONTROL 11

Data Recovery

Safeguards Total 5 — IG1 4/5 — IG2 5/5 — IG3 5/5

Overview

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Why is this Control critical?

In the cybersecurity triad—Confidentiality, Integrity, and Availability (CIA)—the availability of data is, in some cases, more critical than its confidentiality. Enterprises need many types of data to make business decisions, and when that data is not available or is untrusted, then it could impact the enterprise. An easy example is weather information to a transportation enterprise.

When attackers compromise assets, they make changes to configurations, add accounts, and often add software or scripts. These changes are not always easy to identify, as attackers might have corrupted or replaced trusted applications with malicious versions, or the changes might appear to be standard-looking account names. Configuration changes can include adding or changing registry entries, opening ports, turning off security services, deleting logs, or other malicious actions that make a system insecure. These actions do not have to be malicious; human error can cause each of these as well. Therefore, it is important to have an ability to have recent backups or mirrors to recover enterprise assets and data back to a known trusted state.

There has been an exponential rise in ransomware over the last few years. It is not a new threat, though it has become more commercialized and organized as a reliable method for attackers to make money. If an attacker encrypts an enterprise's data and demands ransom for its restoration, having a recent backup to recover to a known, trusted state can be helpful. However, as ransomware has evolved, it has also become an extortion technique, where data is exfiltrated before being encrypted, and the attacker asks for payment to restore the enterprise's data, as well as to keep it from being sold or publicized. In this case, restoration would only solve the issue of restoring systems to a trusted state and continuing operations. Leveraging the guidance within the CIS Controls will help reduce the risk of ransomware through improved cyber hygiene, as attackers usually use older or basic exploits on insecure systems.

Procedures and tools

Data recovery procedures should be defined in the data management process described in CIS Control 3, Data Protection. This should include backup procedures based on data value, sensitivity, or retention requirements. This will assist in developing backup frequency and type (full vs. incremental).

Once per quarter (or whenever a new backup process or technology is introduced), a testing team should evaluate a random sampling of backups and attempt to restore them on a test bed environment. The restored backups should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.

In the event of malware infection, restoration procedures should use a version of the backup that is believed to predate the original infection.

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
11.1	**Establish and Maintain a Data Recovery Process** Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Recover	●	●	●
11.2	**Perform Automated Backups** Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	Data	Recover	●	●	●
11.3	**Protect Recovery Data** Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	Data	Protect	●	●	●
11.4	**Establish and Maintain an Isolated Instance of Recovery Data** Establish and maintain an isolated instance of recovery data. Example implementations include version controlling backup destinations through offline, cloud, or off-site systems or services.	Data	Recover	●	●	●
11.5	**Test Data Recovery** Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.	Data	Recover		●	●

CONTROL 12

Network Infrastructure Management

Safeguards Total	8	IG1	1/8	IG2	7/8	IG3	8/8

Overview

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Why is this Control critical?

Secure network infrastructure is an essential defense against attacks. This includes an appropriate security architecture, addressing vulnerabilities that are, often times, introduced with default settings, monitoring for changes, and reassessment of current configurations. Network infrastructure includes devices such as physical and virtualized gateways, firewalls, wireless access points, routers, and switches.

Default configurations for network devices are geared for ease-of-deployment and ease-of-use—not security. Potential default vulnerabilities include open services and ports, default accounts and passwords (including service accounts), support for older vulnerable protocols, and pre-installation of unneeded software. Attackers search for vulnerable default settings, gaps or inconsistencies in firewall rule sets, routers, and switches and use those holes to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept data while in transmission.

Network security is a constantly changing environment that necessitates regular re-evaluation of architecture diagrams, configurations, access controls, and allowed traffic flows. Attackers take advantage of network device configurations becoming less secure over time as users demand exceptions for specific business needs. Sometimes the exceptions are deployed, but not removed when they are no longer applicable to the business's needs. In some cases, the security risk of an exception is neither properly analyzed nor measured against the associated business need and can change over time.

Procedures and tools

Enterprises should ensure network infrastructure is fully documented and architecture diagrams are kept up-to-date. It is important for key infrastructure components to have vendor support for patches and feature upgrades. Upgrade End-of-Life (EOL) components before the date they will be out of support or apply mitigating controls to isolate them. Enterprises need to monitor their infrastructure versions and configurations for vulnerabilities that would require them to upgrade the network devices to the latest secure and stable version that does not impact the infrastructure.

An up-to-date network architecture diagram, including security architecture diagrams, are an important foundation for infrastructure management. Next is having complete account management for access control, logging, and monitoring. Finally, infrastructure administration should only be performed over secure protocols, with strong authentication (MFA for PAM), and from dedicated administrative devices or out-of-band networks.

Commercial tools can be helpful to evaluate the rule sets of network filtering devices to determine whether they are consistent or in conflict. This provides an automated sanity check of network filters. These tools search for errors in rule sets or Access Controls Lists (ACLs) that may allow unintended services through the network device. Such tools should be run each time significant changes are made to firewall rule sets, router ACLs, or other filtering technologies.

→ **For telework and small office guidance, refer to the CIS Controls Telework and Small Office Network Security Guide –** https://www.cisecurity.org/controls/v8/

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
12.1	**Ensure Network Infrastructure is Up-to-Date** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	Network	Protect	●	●	●
12.2	**Establish and Maintain a Secure Network Architecture** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.	Network	Protect		●	●
12.3	**Securely Manage Network Infrastructure** Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.	Network	Protect		●	●
12.4	**Establish and Maintain Architecture Diagram(s)** Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Network	Identify		●	●
12.5	**Centralize Network Authentication, Authorization, and Auditing (AAA)** Centralize network AAA.	Network	Protect		●	●

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
12.6	**Use of Secure Network Management and Communication Protocols** Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).	Network	Protect		●	●
12.7	**Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure** Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.	Devices	Protect		●	●
12.8	**Establish and Maintain Dedicated Computing Resources for All Administrative Work** Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.	Devices	Protect			●

CONTROL 13

Network Monitoring and Defense

Safeguards Total 11 — IG1 0/11 — IG2 6/11 — IG3 11/11

Overview

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Why is this Control critical?

We cannot rely on network defenses to be perfect. Adversaries continue to evolve and mature, as they share, or sell, information among their community on exploits and bypasses to security controls. Even if security tools work "as advertised," it takes an understanding of the enterprise risk posture to configure, tune, and log them to be effective. Often, misconfigurations due to human error or lack of knowledge of tool capabilities give enterprises a false sense of security.

Security tools can only be effective if they are supporting a process of continuous monitoring that allows staff the ability to be alerted and respond to security incidents quickly. Enterprises that adopt a purely technology-driven approach will also experience more false positives, due to their over-reliance on alerts from tools. Identifying and responding to these threats requires visibility into all threat vectors of the infrastructure and leveraging humans in the process of detection, analysis, and response. It is critical for large or heavily targeted enterprises to have a security operations capability to prevent, detect, and quickly respond to cyber threats before they can impact the enterprise. This process will generate activity reports and metrics that will help enhance security policies, and support regulatory compliance for many enterprises.

As we have seen many times in the press, enterprises have been compromised for weeks, months, or years before discovery. The primary benefit of having comprehensive situational awareness is to increase the speed of detection and response. This is critical to respond quickly when malware is discovered, credentials are stolen, or when sensitive data is compromised to reduce impact to the enterprise.

Through good situational awareness (i.e., security operations), enterprises will identify and catalog Tactics, Techniques, and Procedures (TTPs) of attackers, including their IOCs that will help the enterprise become more proactive in identifying future threats or incidents. Recovery can be achieved faster when the response has access to complete information about the environment and enterprise structure to develop efficient response strategies.

Procedures and tools

Most enterprises do not need to stand up a Security Operations Center (SOC) to gain situational awareness. This starts with first understanding critical business functions, network and server architectures, data and data flows, vendor service and business partner connection, and end-user devices and accounts. This informs the development of a security architecture, technical controls, logging, monitoring, and response procedures.

At the core of this process is a trained and organized team that implements processes for incident detection, analysis, and mitigation. These capabilities could be conducted internally, or through consultants or a managed service provider. Enterprises should consider network, enterprise asset, user credential, and data access activities. Technology will play a crucial role to collect and analyze all of the data, and monitor networks and enterprise assets internally and externally to the enterprise. Enterprises should include visibility to cloud platforms that might not be in line with on-premises security technology.

Forwarding all important logs to analytical programs, such as Security Information and Event Management (SIEM) solutions, can provide value; however, they do not provide a complete picture. Weekly log reviews are necessary to tune thresholds and identify abnormal events. Correlation tools can make audit logs more useful for subsequent manual inspection. These tools are not a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand attacks.

As this process matures, enterprises will create, maintain, and evolve a knowledge base that will help to understand and assess the business risks, developing an internal threat intelligence capability. Threat intelligence is the collection of TTPs from incidents and adversaries. To accomplish this, a situational awareness program will define and evaluate which information sources are relevant to detect, report, and handle attacks. Most mature enterprises can evolve to threat hunting, where trained staff manually review system and user logs, data flows, and traffic patterns to find anomalies.

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
13.1	**Centralize Security Event Alerting** Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.	Network	Detect		●	●
13.2	**Deploy a Host-Based Intrusion Detection Solution** Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.	Devices	Detect		●	●
13.3	**Deploy a Network Intrusion Detection Solution** Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.	Network	Detect		●	●
13.4	**Perform Traffic Filtering Between Network Segments** Perform traffic filtering between network segments, where appropriate.	Network	Protect		●	●

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
13.5	**Manage Access Control for Remote Assets** Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.	Devices	Protect		●	●
13.6	**Collect Network Traffic Flow Logs** Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.	Network	Detect		●	●
13.7	**Deploy a Host-Based Intrusion Prevention Solution** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.	Devices	Protect			●
13.8	**Deploy a Network Intrusion Prevention Solution** Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.	Network	Protect			●
13.9	**Deploy Port-Level Access Control** Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.	Devices	Protect			●
13.10	**Perform Application Layer Filtering** Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.	Network	Protect			●
13.11	**Tune Security Event Alerting Thresholds** Tune security event alerting thresholds monthly, or more frequently.	Network	Detect			●

CONTROL 14

Security Awareness and Skills Training

Safeguards Total	9	IG1	8/9	IG2	9/9	IG3	8/8

Overview

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.

Why is this Control critical?

The actions of people play a critical part in the success or failure of an enterprise's security program. It is 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. Users at every level of the enterprise have different risks. For example: executives manage more sensitive data; system administrators have the ability to control access to systems and applications; and users in finance, human resources, and contracts all have access to different types of sensitive data that can make them targets.

The training should be updated regularly. This will increase the culture of security and discourage risky workarounds.

Procedures and tools

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.

Training should also consider the enterprise's different regulatory and threat posture. Financial firms might have more compliance-related training on data handling and use, healthcare enterprises on handling healthcare data, and merchants for credit card data.

Social engineering training, such as phishing tests, should also include awareness of tactics that target different roles. For example, the financial team will receive BEC attempts posing as executives asking to wire money, or receive emails from compromised partners or vendors asking to change the bank account information for their next payment.

For more comprehensive treatment of this topic, the following resources are helpful to build an effective security awareness program:

- **NIST® SP 800-50 Infosec Awareness Training –** https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf
- **National Cyber Security Centre (UK) –** https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness
- **EDUCAUSE –** https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns
- **National Cyber Security Alliance (NCSA) –** https://staysafeonline.org/
- **SANS –** https://www.sans.org/security-awareness-training/resources
- **For guidance on configuring home routers see the CIS Controls Telework and Small Office Network Security Guide –** https://www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide/

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
14.1	**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.	N/A	Protect	●	●	●
14.2	**Train Workforce Members to Recognize Social Engineering Attacks** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.	N/A	Protect	●	●	●
14.3	**Train Workforce Members on Authentication Best Practices** Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	N/A	Protect	●	●	●
14.4	**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.	N/A	Protect	●	●	●

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
14.5	**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.	N/A	Protect	●	●	●
14.6	**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.	N/A	Protect	●	●	●
14.7	**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.	N/A	Protect	●	●	●
14.8	**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.	N/A	Protect	●	●	●
14.9	**Conduct Role-Specific Security Awareness and Skills Training** Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.	N/A	Protect		●	●

CONTROL 15

Service Provider Management

Safeguards Total 7 | IG1 1/7 | IG2 4/7 | IG3 7/7

Overview

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Why is this Control critical?

In our modern, connected world, enterprises rely on vendors and partners to help manage their data or rely on third-party infrastructure for core applications or functions.

There have been numerous examples where third-party breaches have significantly impacted an enterprise; for example, as early as the late 2000s, payment cards were compromised after attackers infiltrated smaller third-party vendors in the retail industry. More recent examples include ransomware attacks that impact an enterprise indirectly, due to one of their service providers being locked down, causing disruption to business. Or worse, if directly connected, a ransomware attack could encrypt data on the main enterprise.

Most data security and privacy regulations require their protection extend to third-party service providers, such as with Health Insurance Portability and Accountability Act (HIPAA) Business Associate agreements in healthcare, Federal Financial Institutions Examination Council (FFIEC) requirements for the financial industry, and the United Kingdom (U.K.) Cyber Essentials. Third-party trust is a core Governance Risk and Compliance (GRC) function, as risks that are not managed within the enterprise are transferred to entities outside the enterprise.

While reviewing the security of third-parties has been a task performed for decades, there is not a universal standard for assessing security; and, many service providers are being audited by their customers multiple times a month, causing impacts to their own productivity. This is because every enterprise has a different "checklist" or set of standards to grade the service provider. There are only a few industry standards, such as in finance, with the Shared Assessments program, or in higher education, with their Higher Education Community Vendor Assessment Toolkit (HECVAT). Insurance companies selling cybersecurity policies also have their own measurements.

While an enterprise might put a lot of scrutiny into large cloud or application hosting companies because they are hosting their email or critical business applications, smaller firms are often a greater risk. Often times, a third-party service provider contracts with additional parties to provide other plugins or services, such as when a third-party uses a fourth-party platform or product to support the main enterprise.

Procedures and tools

Most enterprises have traditionally used standard checklists, such as ones from ISO 27001 or the CIS Controls. Often, this process is managed through spreadsheets; however, there are online platforms now that allow central management of this process. The focus of this CIS Control though is not on the checklist; instead it is on the fundamentals of the program. Make sure to revisit annually, as relationships and data may change.

No matter what the enterprise's size, there should be a policy about reviewing service providers, an inventory of these vendors, and a risk rating associated with their potential impact to the business in case of an incident. There should also be language in the contracts to hold them accountable if there is an incident that impacts the enterprise.

There are third-party assessment platforms that have an inventory of thousands of service providers, which attempt to provide a central view of the industry, to help enterprises make more informed risk decisions. These platforms often have a dynamic risk score for service providers, based (usually) on passive technical assessments, or enriched through other firms' third-party assessments.

When performing reviews, focus on the services or departments of the provider that are supporting the enterprise. A third-party that has a managed security service contract, or retainer, and holds cybersecurity insurance, can also help with risk reduction.

It is also important to securely decommission service providers when contracts are completed or terminated. Decommission activities may include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

→ **Refer to NIST® 800-88r1: Guidelines for Media Sanitization, as appropriate –** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
15.1	**Establish and Maintain an Inventory of Service Providers** Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify	●	●	●
15.2	**Establish and Maintain a Service Provider Management Policy** Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify		●	●

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
15.3	**Classify Service Providers** Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify		●	●
15.4	**Ensure Service Provider Contracts Include Security Requirements** Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.	N/A	Protect		●	●
15.5	**Assess Service Providers** Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.	N/A	Identify			●
15.6	**Monitor Service Providers** Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.	Data	Detect			●
15.7	**Securely Decommission Service Providers** Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.	Data	Protect			●

CONTROL 16

Application Software Security

Safeguards Total 14 — IG1 0/14 — IG2 11/14 — IG3 14/14

Overview

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Why is this Control critical?

Applications provide a human-friendly interface to allow users to access and manage data in a way that is aligned to business functions. They also minimize the need for users to deal directly with complex (and potentially error-prone) system functions, like logging into a database to insert or modify files. Enterprises use applications to manage their most sensitive data and control access to system resources. Therefore, an attacker can use the application itself to compromise the data, instead of an elaborate network and system hacking sequence that attempts to bypass network security controls and sensors. This is why protecting user credentials (specifically application credentials) defined in CIS Control 6 is so important.

Lacking credentials, application flaws are the attack vector of choice. However, today's applications are developed, operated, and maintained in a highly complex, diverse, and dynamic environment. Applications run on multiple platforms: web, mobile, cloud, etc., with application architectures that are more complex than legacy client-server or database-web server structures. Development life cycles have become shorter, transitioning from months or years in long waterfall methodologies, to DevOps cycles with frequent code updates. Also, applications are rarely created from scratch, and are often "assembled" from a complex mix of development frameworks, libraries, existing code, and new code. There are also modern and evolving data protection regulations dealing with user privacy. These may require compliance to regional or sector-specific data protection requirements.

These factors make traditional approaches to security, like control (of processes, code sources, run-time environment, etc.), inspection, and testing, much more challenging. Also, the risk that an application vulnerability introduces might not be understood, except in a specific operational setting or context.

Application vulnerabilities can be present for many reasons: insecure design, insecure infrastructure, coding mistakes, weak authentication, and failure to test for unusual or unexpected conditions. Attackers can exploit specific vulnerabilities, including buffer overflows, exposure to Structured Query Language (SQL) injection, cross-site scripting, cross-site request forgery, and click-jacking of code to gain access to sensitive data, or take control over vulnerable assets within the infrastructure as a launching point for further attacks.

Applications and websites can also be used to harvest credentials, data, or attempt to install malware onto the users who access them.

Finally, it is now more common to acquire Software as a Service (SaaS) platforms, where software is developed and managed entirely through a third-party. These might be hosted anywhere in the world. This brings challenges to enterprises that need to know what risks they are accepting with using these platforms; and, they often do not have visibility into the development and application security practices of these platforms. Some of these SaaS platforms allow for customizing of their interfaces and databases. Enterprises that extend these applications should follow this CIS Control, similar to if they were doing ground-up customer development.

Procedures and tools

For Version 8, CIS partnered with SAFECode to help develop the procedures and Safeguards for this updated Application Software Security Control. However, application software security is a large topic on its own, and so (consistent with the principles of the overall CIS Controls), we focus here on the most critical Safeguards. These were derived from a companion paper on application software security that SAFECode developed (referenced below), which provides a more in-depth treatment of the topic, and is consistent with SAFECode's existing body of content.

SAFECode developed a three-tiered approach to help readers identify which Development Group (DG) they fit in as a maturity scale for development programs. The three CIS IG levels used within the Safeguards inspired their approach for the DGs below:

Development Group 1

- The enterprise largely relies on off-the-shelf or Open Source Software (OSS) and packages with only the occasional addition of small applications or website coding. The enterprise is capable of applying basic operational and procedural best practices and of managing the security of its vendor-supplied software as a result of following the guidance of the CIS Controls.

Development Group 2

- The enterprise relies on some custom (in-house or contractor-developed) web and/or native code applications integrated with third-party components and runs on-premises or in the cloud. The enterprise has a development staff that applies software development best practices. The enterprise is attentive to the quality and maintenance of third-party open source or commercial code on which it depends.

Development Group 3

- The enterprise makes a major investment in custom software that it requires to run its business and serve its customers. It may host software on its own infrastructure, in the cloud, or both, and may integrate a large range of third-party open source and commercial software components. Software vendors and enterprises that deliver SaaS should consider Development Group 3 as a minimum set of requirements.

The first step in developing an application security program is implementing a vulnerability management process. This process must integrate into the development life cycle, and should be lightweight to insert into the standard bug-fixing progress. The process should include root cause analysis to fix underlying flaws so as to reduce future vulnerabilities, and a severity rating to prioritize remediation efforts.

Developers need to be trained in application security concepts and secure coding practices. This includes a process to acquire or evaluate third-party software, modules, and libraries used in the application to ensure they do not introduce security flaws. The developers should be taught what types of modules they can securely use, where they can be safely acquired, and which components they can, or should not, develop themselves (e.g., encryption).

Weaknesses in the infrastructure that supports these applications can introduce risk. The CIS Controls and the concept of minimizing the attack surface can help secure networks, systems, and accounts that are used within the application. Specific guidance can be found in CIS Controls 1-7, 12, and 13.

The ideal application security program is one that introduces security as early into the software development life cycle as possible. The management of security problems should be consistent and integrated with standard software flaw/bug management, as opposed to a separate process that competes for development resources. Larger or more mature development teams should consider the practice of threat modeling in the design phase. Design-level vulnerabilities are less common than code-level vulnerabilities; however, they often are very severe and much harder to fix quickly. Threat modeling is the process of identifying and addressing application security design flaws before code is created. Threat modeling requires specific training, technical, and business knowledge. It is best conducted through internal "security champions" in each development team, to lead threat modeling practices for that team's software. It also provides valuable context to downstream activities, such as root cause analysis and security testing.

Larger, or commercial, development teams may also consider a bug bounty program where individuals are paid for finding flaws in their applications. Such a program is best used to supplement an in-house secure development process and can provide an efficient mechanism for identifying classes of vulnerabilities that the process needs to focus on.

Finally, in 2020 NIST® published its Secure Software Development Framework (SSDF), which brought together what the industry has learned about software security over the past two decades and created a secure software development framework for planning, evaluating, and communicating about software security activities. Enterprises acquiring software or services can use this framework to build their security requirements and understand whether a software provider's development process follows best practices. These are some application security resources:

- **SAFECode Application Security Addendum –** https://safecode.org/cis-controls/
- **NIST® SSDF –** https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf
- **The Software Alliance –** https://www.bsa.org/reports/updated-bsa-framework-for-secure-software
- **OWASP® –** https://owasp.org/

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
16.1	**Establish and Maintain a Secure Application Development Process** Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect		●	●
16.2	**Establish and Maintain a Process to Accept and Address Software Vulnerabilities** Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.	Applications	Protect		●	●
16.3	**Perform Root Cause Analysis on Security Vulnerabilities** Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.	Applications	Protect		●	●
16.4	**Establish and Manage an Inventory of Third-Party Software Components** Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.	Applications	Protect		●	●
16.5	**Use Up-to-Date and Trusted Third-Party Software Components** Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.	Applications	Protect		●	●
16.6	**Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities** Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.	Applications	Protect		●	●
16.7	**Use Standard Hardening Configuration Templates for Application Infrastructure** Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.	Applications	Protect		●	●
16.8	**Separate Production and Non-Production Systems** Maintain separate environments for production and non-production systems.	Applications	Protect		●	●

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
16.9	**Train Developers in Application Security Concepts and Secure Coding** Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.	Applications	Protect		●	●
16.10	**Apply Secure Design Principles in Application Architectures** Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.	Applications	Protect		●	●
16.11	**Leverage Vetted Modules or Services for Application Security Components** Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.	Applications	Protect		●	●
16.12	**Implement Code-Level Security Checks** Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.	Applications	Protect			●
16.13	**Conduct Application Penetration Testing** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.	Applications	Protect			●
16.14	**Conduct Threat Modeling** Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.	Applications	Protect			●

CONTROL 17

Incident Response Management

Safeguards Total	9	IG1	3/9	IG2	8/9	IG3	9/9

Overview

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Why is this Control critical?

A comprehensive cybersecurity program includes protections, detections, response, and recovery capabilities. Often, the final two get overlooked in immature enterprises, or the response technique to compromised systems is just to re-image them to original state, and move on. The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. Without understanding the full scope of an incident, how it happened, and what can be done to prevent it from happening again, defenders will just be in a perpetual "whack-a-mole" pattern.

We cannot expect our protections to be effective 100% of the time. When an incident occurs, if an enterprise does not have a documented plan—even with good people—it is almost impossible to know the right investigative procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover.

Along with detection, containment, and eradication, communication to stakeholders is key. If we are to reduce the probability of material impact due to a cyber event, the enterprise's leadership must know what potential impact there could be, so that they can help prioritize remediation or restoration decisions that best support the enterprise. These business decisions could be based on regulatory compliance, disclosure rules, service-level agreements with partners or customers, revenue, or mission impacts.

Dwell time from when an attack happens to when it is identified can be days, weeks, or months. The longer the attacker is in the enterprise's infrastructure, the more embedded they become and they will develop more ways to maintain persistent access for when they are eventually discovered. With the rise of ransomware, which is a stable moneymaker for attackers, this dwell time is critical, especially with modern tactics of stealing data before encrypting it for ransom.

Procedures and tools

Even if an enterprise does not have resources to conduct incident response within an enterprise, it is still critical to have a plan. This would include the sources for protections and detections, a list of who to call upon for assistance, and communication plans about how to convey information to leadership, employees, regulators, partners, and customers.

After defining incident response procedures, the incident response team, or a third-party, should engage in periodic scenario-based training, working through a series of attack scenarios fine-tuned to the threats and potential impacts the enterprise faces. These scenarios help ensure that enterprise leadership and technical team members understand their role in the incident response process to help prepare them to handle incidents. It is inevitable that exercise and training scenarios will identify gaps in plans and processes, and unexpected dependencies, which can then be updated into the plan.

More mature enterprises should include threat intelligence and/or threat hunting into their incident response process. This will help the team become more proactive, identifying key or primary attackers to their enterprise or industry to monitor or search for their TTPs. This will help focus detections and define response procedures to identify and remediate more quickly.

The actions in CIS Control 17 provide specific, high-priority steps that can improve enterprise security, and should be a part of any comprehensive incident and response plan. In addition, we recommend the following resource dedicated to this topic:

→ **Council of Registered Security Testers (CREST) Cyber Security Incident Response Guide –** https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf. CREST provides guidance, standards, and knowledge on a wide variety of cyber defense topics.

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
17.1	**Designate Personnel to Manage Incident Handling** Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Respond	●	●	●
17.2	**Establish and Maintain Contact Information for Reporting Security Incidents** Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	N/A	Respond	●	●	●
17.3	**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.	N/A	Respond	●	●	●

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
17.4	**Establish and Maintain an Incident Response Process** Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Respond		●	●
17.5	**Assign Key Roles and Responsibilities** Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Respond		●	●
17.6	**Define Mechanisms for Communicating During Incident Response** Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Respond		●	●
17.7	**Conduct Routine Incident Response Exercises** Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision-making, and workflows. Conduct testing on an annual basis, at a minimum.	N/A	Recover		●	●
17.8	**Conduct Post-Incident Reviews** Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.	N/A	Recover		●	●
17.9	**Establish and Maintain Security Incident Thresholds** Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Recover			●

CONTROL 18

Penetration Testing

Safeguards Total 5 | IG1 0/5 | IG2 3/5 | IG3 5/5

Overview

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Why is this Control critical?

A successful defensive posture requires a comprehensive program of effective policies and governance, strong technical defenses, combined with appropriate action from people. However, it is rarely perfect. In a complex environment where technology is constantly evolving and new attacker tradecraft appears regularly, enterprises should periodically test their controls to identify gaps and to assess their resiliency. This test may be from external network, internal network, application, system, or device perspective. It may include social engineering of users, or physical access control bypasses.

Often, penetration tests are performed for specific purposes:

- As a "dramatic" demonstration of an attack, usually to convince decision-makers of their enterprise's weaknesses
- As a means to test the correct operation of enterprise defenses ("verification")
- To test that the enterprise has built the right defenses in the first place ("validation")

Independent penetration testing can provide valuable and objective insights about the existence of vulnerabilities in enterprise assets and humans, and the efficacy of defenses and mitigating controls to protect against adverse impacts to the enterprise. They are part of a comprehensive, ongoing program of security management and improvement. They can also reveal process weaknesses, such as incomplete or inconsistent configuration management, or end-user training.

Penetration testing differs from vulnerability testing, described in CIS Control 7. Vulnerability testing just checks for presence of known, insecure enterprise assets, and stops there. Penetration testing goes further to exploit those weaknesses to see how far an attacker could get, and what business process or data might be impacted through exploitation of that vulnerability. This is an important detail, and often penetration testing and vulnerability testing are incorrectly used interchangeably. Vulnerability testing is exclusively automated scanning with sometimes manual validation of false

positives, whereas penetration testing requires more human involvement and analysis, sometimes supported through the use of custom tools or scripts. However, vulnerability testing is often a starting point for a penetration test.

Another common term is "Red Team" exercises. These are similar to penetration tests in that vulnerabilities are exploited; however, the difference is the focus. Red Teams simulate specific attacker TTPs to evaluate how an enterprise's environment would withstand an attack from a specific adversary, or category of adversaries.

Procedures and tools

Penetration testing starts with the reconnaissance of the enterprise and environment, and scanning to identify the vulnerabilities that can be used as entries into the enterprise. It is important to make sure all enterprise assets are discovered that are in-scope, and not just rely on a static list, which might be outdated or incomplete. Next, vulnerabilities will be identified in these targets. Exploits to these vulnerabilities are executed to demonstrate specifically how an adversary can either subvert the enterprise's security goals (e.g., the protection of specific sensitive data) or achieve specific adversarial objectives (e.g., the establishment of a covert Command and Control (C2) infrastructure). The results provide deeper insight, through demonstration, into the business risks of various vulnerabilities. This can be against physical access controls, network, system, or application layers, and often includes social engineering components.

Penetration tests are expensive, complex, and potentially introduce their own risks. Experienced people from reputable vendors must conduct them. Some risks include unexpected shutdown of systems that might be unstable, exploits that might delete or corrupt data or configurations, and the output of a testing report that needs to be protected itself, because it gives step-by-step instructions on how to break into the enterprise to target critical assets or data.

Each enterprise should define a clear scope and rules of engagement for penetration testing. The scope of such projects should include, at a minimum, enterprise assets with the highest valued information and production processing functionality. Other lower-value systems may also be tested to see if they can be used as pivot points to compromise higher-value targets. The rules of engagement for penetration test analyses should describe, at a minimum, times of day for testing, duration of test(s), and the overall test approach. Only a few people in the enterprise should know when a penetration test is performed, and a primary point of contact in the enterprise should be designated if problems occur. Increasingly popular recently is having penetration tests conducted through third-party legal counsel to protect the penetration test report from disclosure.

The Safeguards in this CIS Control provide specific, high-priority steps that can improve enterprise security, and should be a part of any penetration testing. In addition, we recommend the use of some of the excellent comprehensive resources dedicated to this topic to support security test planning, management, and reporting:

- **OWASP Penetration Testing Methodologies** – https://www.owasp.org/index.php/Penetration_testing_methodologies
- **PCI Security Standards Council** – https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
18.1	**Establish and Maintain a Penetration Testing Program** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.	N/A	Identify		●	●
18.2	**Perform Periodic External Penetration Tests** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.	Network	Identify		●	●
18.3	**Remediate Penetration Test Findings** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.	Network	Protect		●	●
18.4	**Validate Security Measures** Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.	Network	Protect			●
18.5	**Perform Periodic Internal Penetration Tests** Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.	N/A	Identify			●

Appendix A

Resources and References

Appendix A

Resources and References

CIS Benchmarks™ – http://www.cisecurity.org/cis-benchmarks/

CIS Controls Cloud Companion Guide – https://www.cisecurity.org/controls/v8/

CIS Community Defense Model (CDM) – https://www.cisecurity.org/controls/v8/

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

CIS Controls Assessment Specification – https://controls-assessment-specification.readthedocs.io/en/latest/

CIS Controls Implementation Groups – https://www.cisecurity.org/controls/v8/

CIS Controls Industrial Control Systems Implementation Guide – https://www.cisecurity.org/controls/v8/

CIS Controls Internet of Things Companion Guide – https://www.cisecurity.org/controls/v8/

CIS Controls Mobile Companion Guide – https://www.cisecurity.org/controls/v8/

CIS Controls Self Assessment Tool (CSAT) – https://www.cisecurity.org/controls/cis-controls-self-assessment-tool-cis-csat/

CIS Controls Telework and Small Office Network Security Guide – https://www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide/

CIS Password Policy Guide – https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Risk Assessment Method (RAM) – https://www.cisecurity.org/controls/v8/

Cloud Security Alliance (CSA) – https://cloudsecurityalliance.org/

Council of Registered Security Testers (CREST) Cyber Security Incident Response Guide – CREST provides guidance, standards, and knowledge on a wide variety of cyber defense topics. https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

EDUCAUSE – https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns

International Organization for Standardization – https://www.iso.org/home.html

National Cyber Security Alliance (NCSA) – https://staysafeonline.org/

National Cyber Security Centre (U.K.) – https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness

National Institute of Standards and Technology (NIST®) – https://www.nist.gov/

National Institute of Standards and Technology (NIST®) SSDF – https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf

National Institute of Standards and Technology (NIST®) National Checklist Program Repository – https://nvd.nist.gov/ncp/repository

National Institute of Standards and Technology (NIST®) Digital Identity Guidelines – https://pages.nist.gov/800-63-3/

National Institute of Standards and Technology (NIST®) FIPS 140-2 – https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

National Institute of Standards and Technology (NIST®) FIPS 140-3 – https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

National Institute of Standards and Technology (NIST®) SP 800-50 Infosec Awareness Training – https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

National Institute of Standards and Technology (NIST®) SP 800-88r1—Guidelines for Media Sanitization – https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

National Institute of Standards and Technology (NIST®) SP 800-126r3 The Technical Specification for the Security Content Automation Protocol (SCAP) – https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

OWASP® – https://owasp.org/

OWASP® Penetration Testing Methodologies – https://www.owasp.org/index.php/Penetration_testing_methodologies

PCI Security Standards Council – https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

SAFECode Application Security Addendum – https://safecode.org/cis-controls/

SANS – https://www.sans.org/security-awareness-training/resources

The Software Alliance – https://www.bsa.org/reports/updated-bsa-framework-for-secure-software

Verizon Data Breach Investigations Report – https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Appendix B

Controls and Safeguards Index

Appendix B

Controls and Safeguards Index

Control 01 / Safeguard 1.1 — Control 02 / Safeguard 2.3

CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
01		**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.					
	1.1	**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, data 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.	Devices	Identify	●	●	●
	1.2	**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.	Devices	Respond	●	●	●
	1.3	**Utilize an Active Discovery Tool** Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.	Devices	Detect		●	●
	1.4	**Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory** Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.	Devices	Identify		●	●
	1.5	**Use a Passive Asset Discovery Tool** Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.	Devices	Detect			●
02		**Inventory and Control of Software Assets** Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.					
	2.1	**Establish and Maintain a Software Inventory** Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Applications	Identify	●	●	●
	2.2	**Ensure Authorized Software is Currently Supported** Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Applications	Identify	●	●	●
	2.3	**Address Unauthorized Software** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Applications	Respond	●	●	●

CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
	2.4	**Utilize Automated Software Inventory Tools** Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.	Applications	Detect		●	●
	2.5	**Allowlist Authorized Software** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	Applications	Protect		●	●
	2.6	**Allowlist Authorized Libraries** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.	Applications	Protect		●	●
	2.7	**Allowlist Authorized Scripts** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.	Applications	Protect			●
03		**Data Protection** Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.					
	3.1	**Establish and Maintain a Data Management Process** Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify	●	●	●
	3.2	**Establish and Maintain a Data Inventory** Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	Data	Identify	●	●	●
	3.3	**Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Data	Protect	●	●	●
	3.4	**Enforce Data Retention** Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	Data	Protect	●	●	●
	3.5	**Securely Dispose of Data** Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	Data	Protect	●	●	●
	3.6	**Encrypt Data on End-User Devices** Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Devices	Protect	●	●	●
	3.7	**Establish and Maintain a Data Classification Scheme** Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify		●	●
	3.8	**Document Data Flows** Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Identify		●	●
	3.9	**Encrypt Data on Removable Media** Encrypt data on removable media.	Data	Protect		●	●

CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
	3.10	**Encrypt Sensitive Data in Transit** Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).	Data	Protect		●	●
	3.11	**Encrypt Sensitive Data at Rest** Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.	Data	Protect		●	●
	3.12	**Segment Data Processing and Storage Based on Sensitivity** Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.	Network	Protect		●	●
	3.13	**Deploy a Data Loss Prevention Solution** Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.	Data	Protect			●
	3.14	**Log Sensitive Data Access** Log sensitive data access, including modification and disposal.	Data	Detect			●
04		**Secure Configuration of Enterprise Assets and Software** Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).					
	4.1	**Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect	●	●	●
	4.2	**Establish and Maintain a Secure Configuration Process for Network Infrastructure** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Network	Protect	●	●	●
	4.3	**Configure Automatic Session Locking on Enterprise Assets** Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	Users	Protect	●	●	●
	4.4	**Implement and Manage a Firewall on Servers** Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	Devices	Protect	●	●	●
	4.5	**Implement and Manage a Firewall on End-User Devices** Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Devices	Protect	●	●	●
	4.6	**Securely Manage Enterprise Assets and Software** Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	Network	Protect	●	●	●
	4.7	**Manage Default Accounts on Enterprise Assets and Software** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	Users	Protect	●	●	●

CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
	4.8	**Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.	Devices	Protect		●	●
	4.9	**Configure Trusted DNS Servers on Enterprise Assets** Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.	Devices	Protect		●	●
	4.10	**Enforce Automatic Device Lockout on Portable End-User Devices** Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.	Devices	Respond		●	●
	4.11	**Enforce Remote Wipe Capability on Portable End-User Devices** Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.	Devices	Protect		●	●
	4.12	**Separate Enterprise Workspaces on Mobile End-User Devices** Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.	Devices	Protect			●
05		**Account Management** Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.					
	5.1	**Establish and Maintain an Inventory of Accounts** Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Users	Identify	●	●	●
	5.2	**Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	Users	Protect	●	●	●
	5.3	**Disable Dormant Accounts** Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	Users	Respond	●	●	●
	5.4	**Restrict Administrator Privileges to Dedicated Administrator Accounts** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	Users	Protect	●	●	●
	5.5	**Establish and Maintain an Inventory of Service Accounts** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Users	Identify		●	●
	5.6	**Centralize Account Management** Centralize account management through a directory or identity service.	Users	Protect		●	●

CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3

06 Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

6.1	**Establish an Access Granting Process** Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	Users	Protect	●	●	●
6.2	**Establish an Access Revoking Process** Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	Users	Protect	●	●	●
6.3	**Require MFA for Externally-Exposed Applications** Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	Users	Protect	●	●	●
6.4	**Require MFA for Remote Network Access** Require MFA for remote network access.	Users	Protect	●	●	●
6.5	**Require MFA for Administrative Access** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	Users	Protect	●	●	●
6.6	**Establish and Maintain an Inventory of Authentication and Authorization Systems** Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.	Users	Identify		●	●
6.7	**Centralize Access Control** Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.	Users	Protect		●	●
6.8	**Define and Maintain Role-Based Access Control** Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.	Data	Protect			●

07 Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

7.1	**Establish and Maintain a Vulnerability Management Process** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect	●	●	●
7.2	**Establish and Maintain a Remediation Process** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	Applications	Respond	●	●	●
7.3	**Perform Automated Operating System Patch Management** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Applications	Protect	●	●	●
7.4	**Perform Automated Application Patch Management** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Applications	Protect	●	●	●
7.5	**Perform Automated Vulnerability Scans of Internal Enterprise Assets** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.	Applications	Identify		●	●

CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
	7.6	**Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.	Applications	Identify		●	●
	7.7	**Remediate Detected Vulnerabilities** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.	Applications	Respond		●	●
08		**Audit Log Management** Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.					
	8.1	**Establish and Maintain an Audit Log Management Process** Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Network	Protect	●	●	●
	8.2	**Collect Audit Logs** Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	Network	Detect	●	●	●
	8.3	**Ensure Adequate Audit Log Storage** Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	Network	Protect	●	●	●
	8.4	**Standardize Time Synchronization** Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.	Network	Protect		●	●
	8.5	**Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.	Network	Detect		●	●
	8.6	**Collect DNS Query Audit Logs** Collect DNS query audit logs on enterprise assets, where appropriate and supported.	Network	Detect		●	●
	8.7	**Collect URL Request Audit Logs** Collect URL request audit logs on enterprise assets, where appropriate and supported.	Network	Detect		●	●
	8.8	**Collect Command-Line Audit Logs** Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.	Devices	Detect		●	●
	8.9	**Centralize Audit Logs** Centralize, to the extent possible, audit log collection and retention across enterprise assets.	Network	Detect		●	●
	8.10	**Retain Audit Logs** Retain audit logs across enterprise assets for a minimum of 90 days.	Network	Protect		●	●
	8.11	**Conduct Audit Log Reviews** Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.	Network	Detect		●	●
	8.12	**Collect Service Provider Logs** Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.	Data	Detect			●

CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3

09 Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

9.1	**Ensure Use of Only Fully Supported Browsers and Email Clients**	Applications	Protect	●	●	●
	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.						
9.2	**Use DNS Filtering Services**	Network	Protect	●	●	●
	Use DNS filtering services on all enterprise assets to block access to known malicious domains.						
9.3	**Maintain and Enforce Network-Based URL Filters**	Network	Protect		●	●
	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.						
9.4	**Restrict Unnecessary or Unauthorized Browser and Email Client Extensions**	Applications	Protect		●	●
	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.						
9.5	**Implement DMARC**	Network	Protect		●	●
	To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.						
9.6	**Block Unnecessary File Types**	Network	Protect		●	●
	Block unnecessary file types attempting to enter the enterprise's email gateway.						
9.7	**Deploy and Maintain Email Server Anti-Malware Protections**	Network	Protect			●
	Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.						

10 Malware Defenses

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

10.1	**Deploy and Maintain Anti-Malware Software**	Devices	Protect	●	●	●
	Deploy and maintain anti-malware software on all enterprise assets.						
10.2	**Configure Automatic Anti-Malware Signature Updates**	Devices	Protect	●	●	●
	Configure automatic updates for anti-malware signature files on all enterprise assets.						
10.3	**Disable Autorun and Autoplay for Removable Media**	Devices	Protect	●	●	●
	Disable autorun and autoplay auto-execute functionality for removable media.						
10.4	**Configure Automatic Anti-Malware Scanning of Removable Media**	Devices	Detect		●	●
	Configure anti-malware software to automatically scan removable media.						
10.5	**Enable Anti-Exploitation Features**	Devices	Protect		●	●
	Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.						
10.6	**Centrally Manage Anti-Malware Software**	Devices	Protect		●	●
	Centrally manage anti-malware software.						
10.7	**Use Behavior-Based Anti-Malware Software**	Devices	Detect		●	●
	Use behavior-based anti-malware software.						

CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3

11 Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

11.1	**Establish and Maintain a Data Recovery Process** Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Data	Recover	●	●	●
11.2	**Perform Automated Backups** Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	Data	Recover	●	●	●
11.3	**Protect Recovery Data** Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	Data	Protect	●	●	●
11.4	**Establish and Maintain an Isolated Instance of Recovery Data** Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.	Data	Recover	●	●	●
11.5	**Test Data Recovery** Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.	Data	Recover		●	●

12 Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

12.1	**Ensure Network Infrastructure is Up-to-Date** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	Network	Protect	●	●	●
12.2	**Establish and Maintain a Secure Network Architecture** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.	Network	Protect		●	●
12.3	**Securely Manage Network Infrastructure** Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.	Network	Protect		●	●
12.4	**Establish and Maintain Architecture Diagram(s)** Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Network	Identify		●	●
12.5	**Centralize Network Authentication, Authorization, and Auditing (AAA)** Centralize network AAA.	Network	Protect		●	●
12.6	**Use of Secure Network Management and Communication Protocols** Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).	Network	Protect		●	●
12.7	**Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure** Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.	Devices	Protect		●	●
12.8	**Establish and Maintain Dedicated Computing Resources for All Administrative Work** Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.	Devices	Protect			●

CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3

13 Network Monitoring and Defense

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

13.1	**Centralize Security Event Alerting** Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.	Network	Detect		●	●
13.2	**Deploy a Host-Based Intrusion Detection Solution** Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.	Devices	Detect		●	●
13.3	**Deploy a Network Intrusion Detection Solution** Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.	Network	Detect		●	●
13.4	**Perform Traffic Filtering Between Network Segments** Perform traffic filtering between network segments, where appropriate.	Network	Protect		●	●
13.5	**Manage Access Control for Remote Assets** Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.	Devices	Protect		●	●
13.6	**Collect Network Traffic Flow Logs** Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.	Network	Detect		●	●
13.7	**Deploy a Host-Based Intrusion Prevention Solution** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.	Devices	Protect			●
13.8	**Deploy a Network Intrusion Prevention Solution** Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.	Network	Protect			●
13.9	**Deploy Port-Level Access Control** Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.	Devices	Protect			●
13.10	**Perform Application Layer Filtering** Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.	Network	Protect			●
13.11	**Tune Security Event Alerting Thresholds** Tune security event alerting thresholds monthly, or more frequently.	Network	Detect			●

14 Security Awareness and Skills Training

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.

14.1	**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.	N/A	Protect	●	●	●
14.2	**Train Workforce Members to Recognize Social Engineering Attacks** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.	N/A	Protect	●	●	●

CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
	14.3	**Train Workforce Members on Authentication Best Practices** Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	N/A	Protect	●	●	●
	14.4	**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.	N/A	Protect	●	●	●
	14.5	**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.	N/A	Protect	●	●	●
	14.6	**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.	N/A	Protect	●	●	●
	14.7	**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.	N/A	Protect	●	●	●
	14.8	**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.	N/A	Protect	●	●	●
	14.9	**Conduct Role-Specific Security Awareness and Skills Training** Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.	N/A	Protect	●	●	●
15		**Service Provider Management** Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.					
	15.1	**Establish and Maintain an Inventory of Service Providers** Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify	●	●	●
	15.2	**Establish and Maintain a Service Provider Management Policy** Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify		●	●
	15.3	**Classify Service Providers** Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify		●	●
	15.4	**Ensure Service Provider Contracts Include Security Requirements** Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.	N/A	Protect		●	●

CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
	15.5	**Assess Service Providers** Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.	N/A	Identify			●
	15.6	**Monitor Service Providers** Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.	Data	Detect			●
	15.7	**Securely Decommission Service Providers** Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.	Data	Protect			●
16		**Application Software Security** Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.					
	16.1	**Establish and Maintain a Secure Application Development Process** Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Applications	Protect		●	●
	16.2	**Establish and Maintain a Process to Accept and Address Software Vulnerabilities** Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.	Applications	Protect		●	●
	16.3	**Perform Root Cause Analysis on Security Vulnerabilities** Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.	Applications	Protect		●	●
	16.4	**Establish and Manage an Inventory of Third-Party Software Components** Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.	Applications	Protect		●	●
	16.5	**Use Up-to-Date and Trusted Third-Party Software Components** Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.	Applications	Protect		●	●
	16.6	**Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities** Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.	Applications	Protect		●	●
	16.7	**Use Standard Hardening Configuration Templates for Application Infrastructure** Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.	Applications	Protect		●	●

CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
	16.8	**Separate Production and Non-Production Systems** Maintain separate environments for production and non-production systems.	Applications	Protect		●	●
	16.9	**Train Developers in Application Security Concepts and Secure Coding** Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.	Applications	Protect		●	●
	16.10	**Apply Secure Design Principles in Application Architectures** Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.	Applications	Protect		●	●
	16.11	**Leverage Vetted Modules or Services for Application Security Components** Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.	Applications	Protect		●	●
	16.12	**Implement Code-Level Security Checks** Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.	Applications	Protect			●
	16.13	**Conduct Application Penetration Testing** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.	Applications	Protect			●
	16.14	**Conduct Threat Modeling** Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.	Applications	Protect			●
17		**Incident Response Management** Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.					
	17.1	**Designate Personnel to Manage Incident Handling** Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Respond	●	●	●
	17.2	**Establish and Maintain Contact Information for Reporting Security Incidents** Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	N/A	Respond	●	●	●
	17.3	**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.	N/A	Respond	●	●	●
	17.4	**Establish and Maintain an Incident Response Process** Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Respond		●	●

CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
	17.5	**Assign Key Roles and Responsibilities** Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Respond		●	●
	17.6	**Define Mechanisms for Communicating During Incident Response** Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Respond		●	●
	17.7	**Conduct Routine Incident Response Exercises** Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.	N/A	Recover		●	●
	17.8	**Conduct Post-Incident Reviews** Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.	N/A	Recover		●	●
	17.9	**Establish and Maintain Security Incident Thresholds** Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Recover			●
18		**Penetration Testing** Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.					
	18.1	**Establish and Maintain a Penetration Testing Program** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.	N/A	Identify		●	●
	18.2	**Perform Periodic External Penetration Tests** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.	Network	Identify		●	●
	18.3	**Remediate Penetration Test Findings** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.	Network	Protect		●	●
	18.4	**Validate Security Measures** Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.	Network	Protect			●
	18.5	**Perform Periodic Internal Penetration Tests** Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.	N/A	Identify			●

CIS Center for Internet Security®

CIS Controls®

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats.

Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

To learn more, visit www.CISecurity.org or follow us on Twitter: @CISecurity.

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
CenterforIntSec
TheCISecurity
cisecurity

Redlined

R345, Information Technology Resource Security[1]

R345-1 Purpose: To provide minimum security standards for protecting ~~USHE institutions'~~ Personally Identifiable Information at institutions in the Utah System of Higher Education ("USHE") from potential threats such as human error, accident, system failures, natural disasters, and criminal or malicious action. ~~Specific institutional policies may be more restrictive depending on the security requirements of the institution.~~

R345-2 References

2.1 Board Policy R132, Government Records Access and Management Act Guidelines

2.2 Board Policy R341, Computing Systems Programs

~~**2.3** Board Policy R343, Information Management~~

2.3 Center for Internet Security Critical Security Controls

2.4 Utah Code Title 78B, Chapter 4, Part 7, Cybersecurity Affirmative Defense Act.

2.5 U.S. Department of Homeland Security Handbook for Safeguarding Sensitive PII/Privacy Policy Directive 047-01-007, Revision 3

R345-3 Definitions

~~**3.1 Acceptable Use Policy:** Defines User conduct for appropriate use of the Institution's IT Resources.~~

3.1 ~~The~~ **Center for Internet Security ("CIS") Critical Security Controls:** ~~A~~are a prescriptive, prioritized set of cybersecurity best practices and defensive actions that can help prevent the most pervasive and dangerous attacks, and support compliance in a multi-framework era. These actionable best practices for cyber defense are formulated by a group of IT experts using the information gathered from actual attacks and their effective defenses. The CIS Controls provide specific guidance and a clear pathway for organizations to achieve the goals and objectives described by multiple legal, regulatory, and policy frameworks.

~~**3.2 Administrative Access:** Any account or other access mechanism that permits a Data Steward, Data Custodian, IT Resource administrator, or User to control an IT resource and/or grants functional access to multiple records of Confidential Data.~~

[1] *Adopted March 21, 2008~~;~~ amended September 16, 2016~~, and~~ November 16, 2018, and XXX~~.~~*

Formatted: Font: 26 pt

Formatted: Font: 26 pt

Formatted: Font: Bold

Formatted: Indent: Left: 0.5", First line: 0"

3.2~~3~~ Critical IT Resource~~:~~ ~~A~~is an IT Resource which is required for the continuing operation of the institution and/or its colleges and departments, including any IT Resource which, if it fails to function correctly and/or on schedule, could result in a major failure of mission-critical business functions, a significant loss of funds, or a significant liability or other legal exposure. For example, General Ledger monthly financial reporting may be considered non-Critical IT Resources by the institution, but financial reporting at fiscal year-end may be considered a Critical IT Resource.

~~**3.4 Disaster**: Any event or occurrence that prevents the normal operation of a Critical IT Resource(s).~~

~~**3.5 Disaster Recovery Plan**: A written plan including provisions for implementing and running Critical IT Resources at an alternate site or provisions for equivalent alternate processing (possibly manual) in the event of a disaster.~~

3.3~~6~~ Information Security Office(s) ("ISO")~~:~~ is the office that ~~The Information Security Office~~ develops and maintains security strategies for the institution's IT Resource systems, risk assessments, compliance with ISO policies and guidelines, and for the resolution of campus IT security incidents. The institution may have ISO functions performed by one or more individuals or offices. If multiple individuals or offices are involved, their respective roles and assignments should be clearly delineated.

~~**3.47 Incident Response Team**: A team composed of appropriate campus personnel, including an ISO representative; the Incident Response Team is responsible for immediate response to any breach of security. The Incident Response Team is also responsible for determining and disseminating remedies and preventive measures that develop as a result of responding to and resolving security breaches.~~

Commented [AA1]: This definition is superfluous since these responsibilities are mentioned in section 5 below.

3.4~~5~~8 Information Technology Resource ("IT Resource")~~:~~ means a~~A~~ resource used for electronic storage, processing or transmitting of any data or information, as well as the data or information itself. This definition includes but is not limited to electronic mail, voice mail, local databases, externally accessed databases, Internet-based storage, mobile devices, removable storage, CD-ROM, recorded magnetic media, photographs, digitized information, or microfilm. This also includes any wire, radio, electromagnetic, photo optical, photo electronic or other facility used in transmitting electronic communications, and any computer facilities or related electronic equipment that electronically stores such communications.

3.5~~6~~9 IT Resource Steward~~:~~ means ~~The~~the individual who has policy level responsibility for determining what IT Resources will be stored, who will have access, what security and privacy risk is acceptable, and what measures will be taken to prevent the loss of Information Resources.

3.67~~10~~ IT Resource Custodian~~:~~ means ~~The~~the organization or individual who implements the policy defined by the IT Resource Steward and has responsibility for IT systems that store, process, or transmit IT resources.

3.78~~11~~ IT Resource Administrator~~:~~ means ~~I~~institutional staff that, under the direction of the IT Resource Steward and with operational instructions from the IT Resource Custodian, have day-to-day operational responsibility for data capture, maintenance, and dissemination.

3.89~~12~~ Personally Identifiable Information ("PII")~~: Personally Identifiable Information (PII)~~ is information protected by federal and state laws and regulations, including federal regulations administered by the United States~~.S. the~~ Department of Homeland Security ("DHS"), and is defined by DHS as "any information that permits the identity of an individual to be directly or indirectly inferred, which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual." PII must be protected prior to release in accordance with the Utah Government Records Access Management Act ("GRAMA") or other disclosures required by law. PII includes but is not limited to the following:

Commented [AA2]: This needs a reference to where the definition is located.

3.89~~12~~.1 Full Social Security Number ("SSN")

3.89~~12~~.2 Driver's license or State ID ~~n~~Number

3.89~~12~~.3 Passport ~~n~~Number

3.89~~12~~.4 Visa ~~n~~Number

3.89~~12~~.5 Alien Registration Number

3.89~~12~~.6 Fingerprints or ~~o~~Other ~~b~~Biometric ~~i~~Identifiers

3.89~~12~~.7 Full ~~n~~Name in ~~c~~Combination with:

3.89~~12~~.7.1 Mother's ~~m~~Maiden ~~n~~Name

3.89~~12~~.7.2 Date of ~~b~~Birth

3.89.7.3 Last Four~~4~~ ~~d~~Digits of SSN

Formatted: Font: 10 pt, Bold

3.89~~12~~.7.~~43~~ Citizenship or ~~i~~Immigration ~~s~~Status

3.8912.7.54 Ethnic or rReligious aAffiliation

3.8912.8 Protected Health Information, as defined by the Health Insurance Portability and Accountability Act ("HIPAA").

3.89.913 Personally Identifiable InformationPII does not include "public information" as defined by the Utah Government Records Access and Management Act (GRAMA), or in the case of student records, "directory information" as defined by the Family Education Rights and Privacy Act ("FERPA").

3.904 Security: means Mmeasures taken to reduce the risk of (a) unauthorized access to IT Resources, via either logical, physical, managerial, or social engineering means; and/or (b) damage to or loss of IT Resources through any type of disaster, including cases where in which a violation of security or a disaster occurs despite preventive measures.

3.101 Security Plan: means aA formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Formatted: Font: 10 pt, Not Bold

3.15 Server: A computer used to provide information and/or services to multiple Users.
3.16 Unauthorized Access to IT Resources: Access to Personally Identifiable Information or Critical IT Resources by a User(s) that does not need access to perform his/her job duties.

3.127 User: means Aany person, including a faculty members, staff members, students, patients, and anyone else such as contractors, consultants, interns, and or temporary employees, who accesses and uses institutional IT Resources.

R345-4 Policy: Each institution and its colleges, departments, and divisions, shall take measures to protect Personally Identifiable InformationPII that is stored, processed, or transmitted using IT Resources under their control. Institutions will adopt these measures and review their security methods with the ISO at regular intervals to ensure they are using best practices.

4.1 Institutions shall design reasonable and appropriate security procedures to prevent unauthorized individuals or organizations from accessing IT Resources which store, process, or transmit Personally Identifiable Information.

4.1 Institutions shall adopt and strive to implement the Center for Internet Security (CIS) Critical Security Controls as a guiding security framework and the minimum institutional security standard. Institutions may implement additional frameworks, standards, or regulations as

required by law, contract, or specific circumstances and may be more restrictive than this policy. Each institution shall develop and maintain a written information Security Plan and program informed by the CIS ~~standard~~Critical Security Controls and other applicable requirements.

4.2~~1.1~~ Institutions shall design reasonable and appropriate security procedures informed by their written Security Plan to prevent unauthorized individuals or organizations from accessing ~~for~~ IT Resources that ~~do not~~ store, process, or transmit ~~Personally Identifiable Information~~PII or any ~~if access to such~~ IT Resources that provide~~s~~ a possible vector or avenue to a breach of ~~security of Personally Identifiable Information~~PII or Ceritical IT resources.

4.3. Institutions shall maintain commercial insurance, captive insurance, and/or self-insurance covering loss or breach of ~~Personally Identifiable Information~~PII.

~~**4.1.2** Institutions and departments shall maintain appropriate controls for administrative or functional access to IT resources containing Personally Identifiable Information and shall regularly audit administrative accounts to ensure only currently valid users and administrators have access.~~

~~**4.1.3** Institutions shall implement multi-factor authentication for all administrative and functional access to IT resources that store, process or transmit Personally Identifiable Information.~~

~~**4.1.4** Institutions shall implement on all institutionally-owned computing devices industry-standard encryption that renders the storage media of the device reasonably unrecoverable by a third-party, or other reasonable controls, on any mobile computing or removable storage device that processes, stores, or transmits Personally Identifiable Information.~~

~~**4.1.5** Institutions and departments that entrust Personally Identifiable Information to third-parties (e.g. hosted and/or "cloud" IT Resources) shall review contracts and/or terms of service to ensure the third-party will implement reasonable protections for Personally Identifiable Information in all stages of its lifecycle, including creation, storage, processing, transmittal and destruction.~~

~~**4.1.6** Institutions shall maintain an inventory of all internal or third-party IT Resources that store, process or transmit Personally Identifiable Information.~~

~~**4.2 Preventing the Loss of Critical Institution or Department IT Resources:** At regular intervals using best practices designated by ISO, each institution shall take measures to identify and prevent the loss of Critical IT Resources that are under their control, and to include Critical IT Resources in college, department or division Disaster Recovery Plans.~~

4.3 Protecting PII: Users of IT Resources shall not knowingly retain on personal computers, servers, or other computing devices, Personally Identifiable Information, such as Social Security Numbers; financial information including credit card numbers and bank information; or protected health information, including health records and medical information, except when all of the following conditions are met:

4.3.1 The User needs Personally Identifiable Information to perform duties that are necessary to conduct the business of the institution

4.3.2 The appropriate dean, department chair, or vice president must have granted permission to the User

4.3.3 The institutions have installed industry-standard encryption that renders the storage media of the device reasonably unrecoverable by a third-party, or other reasonable controls, on the user's mobile computing or removable storage device that processes, stores, or transmits Personally Identifiable Information; and

4.3.4 The User must take reasonable precautions to secure the Personally Identifiable Information that resides on his/her personal computer or other computing device.

4.3.5 Permission is not required to retain student grades, letters of recommendation, RPT documents, patentable research findings, etc., that are used regularly in the performance of faculty and staff duties. However, if a computer containing such data is readily accessible to unauthorized individuals, the User must take reasonable precautions to secure the data.

4.4 Preventing the Loss of Critical IT Resources on Users' (Faculty, Staff, Students) IT Resources: A User must take reasonable precautions to reduce the risk of loss of Critical IT Resources that reside on his/her personal computer or other computing device, i.e., at regular intervals backup critical documents on CDs or other media, or back up documents to a storage device or system which is administered by the User's IT Systems Administrator or otherwise approved by the campus for such use.

4.5 Identification of Personally Identifiable Information and Critical IT Resources: If uncertain whether or not an IT Resource contains Personally Identifiable Information or is a Critical IT Resource, a User shall seek direction from the IT Resource Steward, the IT Resource Custodian, the campus Health Insurance Portability and Accountability Act (HIPAA) Privacy Office, or the institution's Information Security Officer.

~~**4.6 Reporting of Security Breaches**: All suspected or actual security breaches of institutional or departmental systems must immediately be reported to the institution's Information Security Officer. IT Systems Administrators should report security incidents to the IT Resource Steward and IT Resource Custodian for their respective organization. If the compromised system contains personal or financial information (e.g. credit card information, Social Security Numbers, etc.), the organization must report the event to the institution's legal office.~~

~~**4.6.1** If an unauthorized person or organization has been accessed or compromised Personally Identifiable Information:~~

~~**4.6.1.1** The IT Resource Steward or User who is responsible for the information must consult with the vice president, dean, department head, supervisor, ISO and the legal office to assess the level of threat and/or liability posed to the institution and to those whose Personally Identifiable Information was accessed.~~

~~**4.6.1.2** The Institution shall notify and direct individuals whose Personally Identifiable Information was accessed or compromised to ISO for instructions regarding measures they should take to protect themselves from identity theft.~~

~~**4.7 Reporting Loss of Critical IT Resource**: If Critical IT Resources are lost, the Data Steward or User must notify those individuals and organizations that are affected by the loss of the resource.~~

~~**4.8 Insurance against Data Loss or Breach**: Institutions shall maintain an insurance policy covering loss or breach of Personally Identifiable Information.~~

~~**4.9 Physical Security**: Users are responsible for assuring that all electronic information, hard copy information, and hardware devices in their possession are physically protected in accordance with their classification level at all times. Users shall follow at all times the security controls for each work area and that they comply with access restrictions, sensitive data handling procedures, and the security plan for each area.~~

~~**4.10 Destruction or "Wiping" of Electronic Media**: Departments and Users shall destroy Personally Identifiable Information as well as other personal or financial information in a campus IT Resource or on personal computers, servers, or other campus computing devices, when such information is no longer needed to conduct the business of the institution, using established institutional procedures.~~

R345-5 Roles and Responsibilities: Each institution shall clearly define the roles and responsibilities of persons charged with the security of institutional information resources. The ~~institution may organize~~

~~the~~ ISO office(s) at an institution may be comprised of one or more persons or groups ~~as one person or multiple groups to fit~~based on the institution's IT Security ~~its~~ needs. ~~Also, t~~The institution may also choose to use designations other than "IT Resource Steward, IT Resource Custodian, and IT Resource ~~-~~Administrators" to describe the persons charged with the following roles and responsibilities.

5.1 Institutional ~~Information Security Office(s) (~~ISO~~)~~: The ISO reports directly to a senior institutional administrator. The ISO is responsible ~~for the~~to coordinat~~e~~ion, review, and approv~~e~~al ~~of~~ procedures used to provide the requisite security for ~~Personally Identifiable Information~~PII or Critical IT Resources. The ISO is also responsible for coordinating compliance with this policy and shall:

5.1.1 Implement and enforce adherence to the CIS Critical Security Controls;~~.~~

5.1.2~~1~~ Develop and maintain security policies, plans, procedures, strategies, architectures, best practices, and minimum requirements;~~.~~

5.1.3 Provide guidance consistent with institutional policy to IT Resource Stewards and IT Resource Custodians;~~.~~

5.1.4 Operate or coordinate the operation of technical security controls and security systems;~~.~~

~~**5.1.2** Educate and provide assistance in complying with this policy to IT Resource Stewards, IT Resource Custodians, IT Resource Administrators, and Users. Provide guidelines consistent with institutional policies, consultation, and assistance to campus departments and individuals regarding the proper use of computer workstations, servers, applications, group networks and other IT Resources.~~

~~**5.1.3** Implement and enforce baseline perimeter security practices endorsed for institutions by federal, state, and local government agencies, and national organizations such as Educause, the SANS Institute, and the National Institute of Standards and Technology.~~

~~**5.1.4** Monitor and analyze campus network traffic information to ensure compliance with institutional security and acceptable use policies, and evaluate, identify, and resolve security vulnerabilities, breaches and threats to the institution's IT Resources.~~

5.1.5 Conduct periodic and ongoing security audits ~~ongoing, periodic~~ to confirm compliance with this policy;~~.~~

5.1.6 Direct the campus Incident Response Team, incident response activities, and incident resolution at institutional, departmental, and individual levels, and. Ttake appropriate and reasonable remedial action to resolve security incidents;.

5.1.7 Assist institutional or third-party auditors in the analysis of campus IT Resources to further ensure policy compliance; and.

5.1.8 Monitor compliance with security policies and procedures and report compliance violations to the relevant cognizant authority.

5.2 IT Resource Custodian: IT Resource Custodians (Computer Services and other IT Resources related work units or individuals) will manage the campus backbone network and other IT systems and resources and, as related to their security roles and responsibilities, shall:

5.2.1 Monitor the campus network traffic flows, primarily for the purpose of network maintenance and optimization.

5.2.1 Implement and administer the security of IT Resources in accordance with the CIS Controls;.

5.2.2 Inform the Information Security Officer of indicators of attacktraffic patterns, which pursuant to best practices, procedures, and standards, may indicate a potential or actual threat to the network backbone and campus IT Resources; and.

5.2.3 Apply security policy and procedures to IT Resources campus network devices as directed by the ISO.

5.3 Incident Response Team: Under the direction of the Information Security Officer, the Incident Response Team is responsible for immediate response to any breach of security. The Incident Response TeamThis team is also responsible for determining and disseminating remedies and preventative measures that develop as a result of responding to and resolving security breaches.

5.4 IT Resource Steward: The IT Resource Steward is designated by the cognizant authority of the relevant group or work unit, is familiar with data issues, laws, and regulations., and shall:

5.4.1 The IT Resource Steward shall:

5.4.1.1 Determine the purpose and function of the IT Resource;.

5.4.1.2 Determine the level of security required based on the sensitivity of the IT Resource;.

5.4.1.3 Determine the criticality of ~~how critical~~ the IT Resource;.

5.4.1.4 Determine accessibility rights to the IT Resource;.

5.4.1.5 Determine the appropriate method for providing business continuity for Critical IT Resources (e.g., performing s~~S~~ervice c~~C~~ontinuity at an alternate site, performing equivalent manual procedures, etc.); and.

5.4.1.6 Specify adequate data retention, in accordance with the institution's policies, and state and federal laws for IT Resources consisting of applications or data.

~~**5.4.7** Monitor and analyze network traffic and system log information for the purpose of evaluating, identifying and resolving security breaches and/or threats to the IT Resources of the organization for which they have responsibility.~~

5.4.2~~78~~ An IT Resource Steward in a work unit that lacks the professional IT staff or expertise to accomplish items 5.4.1 through 5.4.7, or to fulfill the responsibilities of the IT Resource Administrators, may request assistance from the Information Security Officer.

5.5 IT Resource Administrator: The IT Resource Administrator(s) performs security functions and procedures as directed by the IT Resource Steward, and implement~~sing~~ and administer~~sing~~ the security of IT Resources in accordance with institutional policy and industry best practices and standards.

R345-6 Sanctions and Remedies

6.1 Emergency Action by the ISO: The ISO may discontinue service to any User who violates this policy or other IT policies when continuation of ~~such~~ the service threatens the security (including integrity, privacy, and availability) of the institution's IT Resources. The ISO may also discontinue service to any network segment or networked device if the continued operation of such segments or devices threatens the security of the institution's IT Resources. Unless non-compliance is causing a direct and imminent threat to the institution's IT Resources necessitating emergency action, ~~The~~the ISO will notify the IT Resource Steward or ~~his/her~~their designee to assist ~~in the resolution~~with resolving ~~of~~ non-compliance issues before discontinuing service(s) ~~are discontinued, unless non-compliance is causing a direct and imminent threat to the institution's IT Resources~~.

6.2 Emergency Action by the IT Resource Steward: The IT Resource Steward may discontinue service or request that the ISO discontinue service to network segments, network devices, or Users under ~~his or her~~their jurisdiction, ~~which~~ that are not in compliance with this policy. Unless non-compliance is causing a direct and imminent threat to the institution's IT Resources necessitating emergency action, the IT Resource Steward~~s~~ will notify, or request that the ISO notify, affected individuals to assist ~~in the resolution of~~with resolving non-compliance issues before discontinuing service(s) ~~are discontinued~~, ~~unless non-compliance is causing a direct and imminent threat to the institution's IT Resources.~~

6.3 Restoration of Access: A User's access may be restored as soon as the direct and imminent security threat has been remedied.

6.4 Revocation of Access: USHE institutions shall reserve the right to revoke access to any IT Resource for any User who violates the institution's policy, or for any other business reasons as allowed by applicable institutional policies.

6.5 Disciplinary Action: Violation of the institution's policy may result in disciplinary action, including termination of employment. Employees ~~Staff members~~ may appeal revocation of access to IT Resources or disciplinary actions taken against them pursuant to institutional policy.

R345, Information Technology Resource Security[1]

R345-1 Purpose: To provide minimum security standards for protecting Personally Identifiable Information at institutions in the Utah System of Higher Education ("USHE") from potential threats such as human error, accident, system failures, natural disasters, and criminal or malicious action.

R345-2 References

2.1 Board Policy R132, Government Records Access and Management Act Guidelines

2.2 Board Policy R341, Computing Systems Programs

2.3 Center for Internet Security Critical Security Controls

2.4 Utah Code Title 78B, Chapter 4, Part 7, Cybersecurity Affirmative Defense Act.

2.5 U. S. Department of Homeland Security Handbook for Safeguarding Sensitive PII/Privacy Policy Directive 047-01-007, Revision 3

R345-3 Definitions

3.1 Center for Internet Security ("CIS") Critical Security Controls are a prescriptive, prioritized set of cybersecurity best practices and defensive actions that can help prevent the most pervasive and dangerous attacks, and support compliance in a multi-framework era. These actionable best practices for cyber defense are formulated by a group of IT experts using the information gathered from actual attacks and their effective defenses. The CIS Controls provide specific guidance and a clear pathway for organizations to achieve the goals and objectives described by multiple legal, regulatory, and policy frameworks.

3.2 Critical IT Resource is an IT Resource which is required for the continuing operation of the institution and/or its colleges and departments, including any IT Resource which, if it fails to function correctly and/or on schedule, could result in a major failure of mission-critical business functions, a significant loss of funds, or a significant liability or other legal exposure. For example, General Ledger monthly financial reporting may be considered non-Critical IT Resources by the institution, but financial reporting at fiscal year-end may be considered a Critical IT Resource.

[1] *Adopted March 21, 2008; amended September 16, 2016, November 16, 2018, and XXX*

3.3 Information Security Office(s) ("ISO") is the office that develops and maintains security strategies for the institution's IT Resource systems, risk assessments, compliance with ISO policies and guidelines, and for the resolution of campus IT security incidents. The institution may have ISO functions performed by one or more individuals or offices. If multiple individuals or offices are involved, their respective roles and assignments should be clearly delineated.

3.4 Information Technology Resource ("IT Resource") means a resource used for electronic storage, processing or transmitting of any data or information, as well as the data or information itself. This definition includes but is not limited to electronic mail, voice mail, local databases, externally accessed databases, Internet-based storage, mobile devices, removable storage, CD-ROM, recorded magnetic media, photographs, digitized information, or microfilm. This also includes any wire, radio, electromagnetic, photo optical, photo electronic or other facility used in transmitting electronic communications, and any computer facilities or related electronic equipment that electronically stores such communications.

3.5 IT Resource Steward means the individual who has policy level responsibility for determining what IT Resources will be stored, who will have access, what security and privacy risk is acceptable, and what measures will be taken to prevent the loss of Information Resources.

3.6 IT Resource Custodian means the organization or individual who implements the policy defined by the IT Resource Steward and has responsibility for IT systems that store, process, or transmit IT resources.

3.7 IT Resource Administrator means institutional staff that, under the direction of the IT Resource Steward and with operational instructions from the IT Resource Custodian, have day-to-day operational responsibility for data capture, maintenance, and dissemination.

3.8 Personally Identifiable Information ("PII") is information protected by federal and state laws and regulations, including federal regulations administered by the United States Department of Homeland Security ("DHS"), and is defined by DHS as "any information that permits the identity of an individual to be directly or indirectly inferred, which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual." PII must be protected prior to release in accordance with the Utah Government Records Access Management Act ("GRAMA") or other disclosures required by law. PII includes but is not limited to the following:

3.8.1 Full Social Security Number ("SSN")

3.8.2 Driver's license or State ID Number

3.8.3 Passport Number

3.8.4 Visa Number

3.8.5 Alien Registration Number

3.8.6 Fingerprints or Other Biometric Identifiers

3.8.7 Full Name in Combination with:

3.8.7.1 Mother's Maiden Name

3.8.7.2 Date of Birth

3.8.7.3 Last Four Digits of SSN

3.8.7.4 Citizenship or Immigration Status

3.8.7.5 Ethnic or Religious Affiliation

3.8.8 Protected Health Information, as defined by the Health Insurance Portability and Accountability Act ("HIPAA").

3.8.9 PII does not include "public information" as defined by GRAMA, or in the case of student records, "directory information" as defined by the Family Education Rights and Privacy Act ("FERPA").

3.9 Security means measures taken to reduce the risk of (a) unauthorized access to IT Resources, via either logical, physical, managerial, or social engineering means; and/or (b) damage to or loss of IT Resources through any type of disaster, including cases in which a violation of security or a disaster occurs despite preventive measures.

3.10 Security Plan means a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

3.11 User means any person, including a faculty member, staff member, student, patient, contractor, consultant, intern, or temporary employee, who accesses and uses institutional IT Resources.

R345-4 Policy: Each institution and its colleges, departments, and divisions shall take measures to protect PII that is stored, processed, or transmitted using IT Resources under their control.

4.1 Institutions shall adopt and strive to implement the CIS Critical Security Controls as a guiding security framework and the minimum institutional security standard. Institutions may implement additional frameworks, standards, or regulations as required by law, contract, or specific circumstances and may be more restrictive than this policy. Each institution shall develop and maintain a written information Security Plan and program informed by the CIS Critical Security Controls and other applicable requirements.

4.2 Institutions shall design reasonable and appropriate security procedures informed by their written Security Plan to prevent unauthorized individuals or organizations from accessing IT Resources that store, process, or transmit PII or any IT Resources that provide a possible vector or avenue to a breach of PII or Critical IT resources.

4.3. Institutions shall maintain commercial insurance, captive insurance, and/or self-insurance covering loss or breach of PII.

R345-5 Roles and Responsibilities: Each institution shall clearly define the roles and responsibilities of persons charged with the security of institutional information resources. The ISO office(s) at an institution may be comprised of one or more persons or groups based on the institution's IT Security needs. The institution may also choose to use designations other than "IT Resource Steward, IT Resource Custodian, and IT Resource
Administrators" to describe the persons charged with the following roles and responsibilities.

5.1 Institutional ISO: The ISO reports directly to a senior institutional administrator. The ISO is responsible to coordinate, review, and approve procedures used to provide the requisite security for PII or Critical IT Resources. The ISO is also responsible for coordinating compliance with this policy and shall:

5.1.1 Implement and enforce adherence to the CIS Critical Security Controls;

5.1.2 Develop and maintain security policies, plans, procedures, strategies, architectures, best practices, and minimum requirements;

5.1.3 Provide guidance consistent with institutional policy to IT Resource Stewards and IT Resource Custodians;

5.1.4 Operate or coordinate the operation of technical security controls and security systems;

5.1.5 Conduct periodic and ongoing security audits to confirm compliance with this policy;

5.1.6 Direct the campus Incident Response Team, incident response activities, and incident resolution at institutional, departmental, and individual levels, and take appropriate and reasonable remedial action to resolve security incidents;

5.1.7 Assist institutional or third-party auditors in the analysis of campus IT Resources to further ensure policy compliance; and

5.1.8 Monitor compliance with security policies and procedures and report compliance violations to the relevant cognizant authority.

5.2 IT Resource Custodian: IT Resource Custodians (Computer Services and other IT Resources related work units or individuals) will manage the campus network and other IT systems and resources and, as related to their security roles and responsibilities, shall:

5.2.1 Implement and administer the security of IT Resources in accordance with the CIS Controls;

5.2.2 Inform the Information Security Officer of indicators of attack, which pursuant to best practices, procedures, and standards, may indicate a potential or actual threat to the network and campus IT Resources; and

5.2.3 Apply security policy and procedures to IT Resources as directed by the ISO.

5.3 Incident Response Team: Under the direction of the Information Security Officer, the Incident Response Team is responsible for immediate response to any breach of security. This team is also responsible for determining and disseminating remedies and preventative measures that develop as a result of responding to and resolving security breaches.

5.4 IT Resource Steward: The IT Resource Steward is designated by the cognizant authority of the relevant group or work unit, is familiar with data issues, laws, and regulations.

5.4.1 The IT Resource Steward shall:

5.4.1.1 Determine the purpose and function of the IT Resource;

5.4.1.2 Determine the level of security required based on the sensitivity of the IT Resource;

5.4.1.3 Determine the criticality of the IT Resource;

5.4.1.4 Determine accessibility rights to the IT Resource;

5.4.1.5 Determine the appropriate method for providing business continuity for Critical IT Resources (e.g., performing service continuity at an alternate site, performing equivalent manual procedures, etc.); and

5.4.1.6 Specify adequate data retention, in accordance with the institution's policies, and state and federal laws for IT Resources consisting of applications or data.

5.4.2 An IT Resource Steward in a work unit that lacks the professional IT staff or expertise to accomplish items 5.4.1 through 5.4.7, or to fulfill the responsibilities of the IT Resource Administrators, may request assistance from the Information Security Officer.

5.5 IT Resource Administrator: The IT Resource Administrator(s) performs security functions and procedures as directed by the IT Resource Steward, and implements and administers the security of IT Resources in accordance with institutional policy and industry best practices and standards.

R345-6 Sanctions and Remedies

6.1 Emergency Action by the ISO: The ISO may discontinue service to any User who violates this policy or other IT policies when continuation of the service threatens the security (including integrity, privacy, and availability) of the institution's IT Resources. The ISO may also discontinue service to any network segment or networked device if the continued operation of such segments or devices threatens the security of the institution's IT Resources. Unless non-compliance is causing a direct and imminent threat to the institution's IT Resources necessitating emergency action, the ISO will notify the IT Resource Steward or their designee to assist with resolving non-compliance issues before discontinuing service(s).

6.2 Emergency Action by the IT Resource Steward: The IT Resource Steward may discontinue service or request that the ISO discontinue service to network segments, network devices, or Users under their jurisdiction, that are not in compliance with this policy. Unless non-compliance is causing a direct and imminent threat to the institution's IT Resources necessitating emergency action, the IT Resource Steward will notify, or request that the ISO notify, affected individuals to assist with resolving non-compliance issues before discontinuing service(s),

6.3 Restoration of Access: A User's access may be restored as soon as the direct and imminent security threat has been remedied.

6.4 Revocation of Access: USHE institutions shall reserve the right to revoke access to any IT Resource for any User who violates the institution's policy, or for any other business reasons as allowed by applicable institutional policies.

6.5 Disciplinary Action: Violation of the institution's policy may result in disciplinary action, including termination of employment. Employees may appeal revocation of access to IT Resources or disciplinary actions taken against them pursuant to institutional policy.