CIS Center for Internet Security®

CIS Controls

Privacy Companion Guide

January 2022

Acknowledgments

The Center for Internet Security® (CIS®) would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls® (CIS Controls®) and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editors
Joshua M. Franklin, CIS
Christina Runnegar, Internet Society

Contributors
Ginger Anderson, CIS
Michael Felt, IBM
Alexis Hancock, Electronic Frontier Foundation
Robin Regnier, CIS
Tony Rutowski, ETSI
Valecia Stocchetti, CIS
and other expert volunteers from the CIS Community for the content and editing of this guide.

Contents

Introduction

The CIS Critical Security Controls (CIS Controls) are a prioritized set of actions that collectively form a defense-in-depth approach and best practices to mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of information technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors, including retail, manufacturing, healthcare, transportation, education, government, defense, and others. While the CIS Controls address the general practices that most enterprises should take to secure their systems, some operational environments and aspects of an information security program may present unique requirements not addressed by the CIS Controls.

Many professionals within the cybersecurity industry struggle to understand the differences between privacy and security. Some view both as an interrelated means to an end, such as privacy is provided through the use of encryption to protect confidentiality. Some IT professionals also equate "privacy" with confidentiality. This confusion makes it challenging for IT professionals to protect privacy effectively, since it's often impractical to achieve privacy without security; however, it is possible to obtain security without privacy. Or worse, security can be achieved at the expense of privacy. Additionally, legal staff grapple with the implications of changes in technology that often outpace the law. The purpose of the *CIS Controls Privacy Guide* is to develop best practices and guidance for implementing the CIS Controls while carefully considering the privacy impacts on the workforce, customers, and third-parties. The *Privacy Guide* supports the objectives of the CIS Controls by aligning privacy principles and highlighting potential privacy concerns that may arise through the usage of the CIS Controls. Considerations are presented so that IT, legal, and any other staff with privacy responsibilities can identify opportunities to integrate privacy considerations into data security controls.

Methodology

A consistent approach is needed for analyzing the CIS Controls in the context of privacy. CIS is leveraging the Fair Information Practice Principles (FIPPs)[1] and the General Data Protection Regulation (GDPR)[2] to help analyze the privacy implications of each CIS Control.

The FIPPs are directly quoted as follows:

1. **The Collection Limitation Principle.** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **The Data Quality Principle.** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. **The Purpose Specification Principle.** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **The Use Limitation Principle.** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except a) with the consent of the data subject, or b) by the authority of law.
5. **The Security Safeguards Principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. **The Openness Principle.** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **The Individual Participation Principle.** An individual should have the right:
    a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
    b. to have data relating to him communicated to him, within a reasonable time, at a charge, if any, that is not excessive; in a reasonable manner, and in a form that is readily intelligible to him;
    c. to be given reasons if a request made under subparagraphs (a) and (b) is denied and to be able to challenge such denial; and
    d. to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
8. **The Accountability Principle.** A data controller should be accountable for complying with measures which give effect to the principles stated above.

1 Fair Information Practice Principles (iapp.org)
2 General Data Protection Regulation (gdpr.eu)

GDPR is a multifaceted regulation governing the processing of personal data, as well as other technical aspects of an enterprise, in the European Union (EU) and beyond. The essential characteristics of the regulation are to protect personal data as a fundamental right and that privacy is to be respected. Many new privacy laws across the world are using the GDPR as framework for privacy law in their own country, state, or region. The EU wrote GDPR in such a way so that it applies to any enterprise that processes the data of EU citizens. Therefore, each CIS Control is analyzed for steps enterprises would need to take in order to ensure that they are including GDPR principles in their business. This is not to say that implementing each CIS Control will make an enterprise compliant with GDPR.

Since GDPR is large law, spanning multiple areas, CIS has highlighted the areas of GDPR to be covered by this guide below.[3]

1. **Lawfulness, fairness, and transparency:** processed lawfully, fairly and in a transparent manner in relation to the data subject.
2. **Purpose limitation:** collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.
3. **Data minimization:** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy of data:** accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. **Storage limitation:** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational [sic] measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.
6. **Integrity and confidentiality:** processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised [sic] or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational [sic] measures.

These are only the principles of GDPR. GDPR also declares a number of rights for users, with some of these being somewhat new concepts. This includes the right to erasure ("right to be forgotten"), which allows a user to request that their data be deleted from a data owner if certain conditions are met. Other rights include the ability for users to access their own data and to correct inaccuracies. In addition to rights for users, stipulations are put onto EU companies such as mandatory breach notifications if a company suffers a data breach and designing all future products from companies to leverage privacy as a foundational principle. GDPR contains too many items to analyze in this single document, and this guide will focus on GDPR Principles 1–6.

3 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1797-1-1

Document Structure

For each of the 18 CIS Controls, the following information is provided in this document:

- **Privacy Applicability –** Explores the degree to which a CIS Control pertains to privacy. Only specific Safeguards within a Control contribute towards privacy. This could include protecting the privacy of employees and customers, but may also include the enterprise's IT systems.
- **Privacy Implications –** Includes the privacy issues and/or risks associated with implementing specific CIS Controls. This helps implement the Use Limitation, Security Safeguards, and Accountability FIPPs.
    - **Data Collection –** This focuses on the types of data collected by the enterprise when implementing a CIS Control. While there is always a specific focus on personally identifiable information (PII), other data types may also be assessed such as open data, commercial data, and customer data (e.g., information about individuals using a company's services).
    - **Data Storage –** After data is collected, it must be stored somewhere until it is deleted. This portion analyzes issues associated with storing data such as where and how data is stored. This also includes the parties involved in the storage process.
- **Additional Discussion –** A general guidance area to include relevant tools, products, or threat information that could be of use can be found here. This helps implement the Purpose Specification and Data Quality and Integrity and confidentiality FIPPs.
- **Fair Information Practice Principles –** Concerns and other information associated with the FIPPs principles. Only relevant FIPPs will be listed.
- **General Data Protection Regulation Principles –** Concerns and other information associated with the GDPR principles. Only pre-specified GDPR principles will be listed.

Additionally, a **Control Applicability Table** is provided at the end of every section. This table shows the applicability of each CIS Safeguard to privacy. The letter "Y" shows that a CIS Safeguard has privacy impacts, and "N" means there is no privacy impact. These tables notate any privacy impacts a particular CIS Safeguard may have and can assist in privacy engineering efforts. At times it was difficult to identify when a Safeguard was directly applicable to privacy. For instance, many Safeguards are designed to keep information secure from unauthorized disclosure via uses of cryptography and access control. But when identifying if a Safeguard is applicable to privacy, evaluating if a Control can protect the security of personal data was ultimately not a consideration. If it was a consideration, then all of the Safeguards within the CIS Controls would be applicable as they are designed to secure the IT systems which hold the personal data.

Audience

This *Privacy Guide* is a resource meant for both IT security professionals, who are familiar with the CIS Controls, and privacy or legal staff within an enterprise. Users of this guide should have a working knowledge of basic privacy concepts. The previously introduced FIPPs in many ways are a foundational element in the privacy space. This document provides a history of their development and usage. The National Institute of Standards and Technology (NIST®) Privacy Framework provides a baseline guide to privacy concepts. Finally, certifications such as the Certified Information Privacy Professional (CIPP) from the International Association of Privacy Professionals (IAPP) can assist professionals in learning to understand the core concepts of privacy engineering and managing privacy risk.

This document provides a bridge between IT security professionals looking to better understand how privacy applies to IT security controls, and privacy or legal professionals who need to better understand how modern technology and IT processes might impact privacy. Hopefully this document can enable a line of communication between these two groups and enhance the overall governance process by which business and legal management communicate with IT and IT security teams. Proper data governance will help enterprises better understand the privacy implications associated with implementing specific CIS Controls, and potentially develop additional mitigations to assist with meeting an enterprise's privacy objectives.

We hope that privacy professionals learn about the CIS Controls and how they can be a tool to support privacy requirements. This guide should be a good starting point to establish a constructive dialogue and cooperation among all groups. The Privacy Guide is useful for enterprises of any size: large enterprises that might lack solid communication between IT and legal teams and Small/Medium Enterprises (SMEs) that might not know what they need to know. The guide outlines some of the privacy implications of the CIS Controls and suggests mitigation approaches. Technical staff may not be aware of topics like regulatory requirements, data protection standards, requirements within partner agreements, and breach disclosure laws, which they need to prepare for reporting. There is no silver bullet to approaching privacy considerations as they are often complex and will vary by country, state, industry, customer type, and other factors.

Scope

While a complete treatment of privacy could be quite lengthy, this guide is only meant as a starting point to outline the most essential processes that every enterprise should focus on when dealing with data privacy and security concerns. Although the following topics fall outside the scope of the guide, we encourage enterprises to be mindful of the following issues, where applicable:

- Evolving national and international privacy laws
- Breach disclosure requirements that are locally, regionally, or nationally applicable including any other breach disclosure laws unique to an industry or sector
- Privacy related to personal mobile devices used in the enterprise
- Privacy related to leveraging another enterprise's platform or service (e.g., cloud computing)
- Data created as a result of using products and services of another company that could impact the privacy of employees and users
- Data portability requirements
- International transfers

In noting privacy implications of the CIS Controls and suggesting mitigations, this document takes a broad view of privacy, since laws vary. As such, it is critical that IT security and privacy teams work in tandem to achieve both regulatory and internal privacy goals.

Finally, in the context of this guide, privacy was considered for employees and the customers of products and services made by the enterprise. Essentially, privacy for employees from the enterprise was considered, and also privacy for end-users from having their passwords posted online.

Privacy Assessments

There are many ways to assess how privacy is protected within an enterprise. The National Academy of Sciences (NAS) Privacy Research and Best Practices report[4] states that, *"organizations must develop and continuously adapt their own internal policies and practices to protect privacy—beyond those that are legally mandated—in order to be effective and maintain the trust of their stakeholders and the public."* Therefore, CIS encourages enterprises to engage in a privacy assessment when implementing new IT systems or controls. Many privacy assessment frameworks exist and are based on different but often related foundational principles.

A Privacy Impact Assessment (PIA) is one way of performing privacy assessments. PIAs help an enterprise identify personal data that an enterprise collects, processes, shares, and maintains. They can assist in demonstrating that program managers and system owners intentionally incorporate privacy principles throughout their information systems and business practices. There are multiple ways to perform a privacy impact assessment. The Government of New Zealand published a document providing useful steps for performing a privacy impact assessment.

NIST provides a Privacy Framework that is a more recent approach for assessing privacy within an enterprise. The framework is a *"tool that can help your enterprise create or improve a privacy program. Effective privacy risk management can help you build trust in your products and services, communicate better about your privacy practices, and meet your compliance obligations. Good cybersecurity is important but can't address all privacy risks."* NIST® provides several resources to help small and medium-sized enterprises to incorporate privacy principles into their current IT practices.

Finally, the European Telecommunications Standards Institute (ETSI) has provided resources for privacy enhancing implementations using the CIS Controls via ETSI TR 103 305-5. There are a variety of mechanisms within this document that can facilitate and encourage privacy protection. In addition, the Controls can help meet provisions of the EU General Data Protection Regulation (GDPR) using the CIS Critical Security Controls. The present document is directed at both achieving privacy objectives and performing privacy impact assessments.

The CIS Controls do not contain a Control specifically focusing on privacy. As such, CIS does not recommend a single approach for performing a privacy assessment. Instead, multiple approaches are provided to make end-users aware of the options that exist to facilitate increasing privacy mechanisms.

4 National Academies of Sciences, Engineering, and Medicine. 2016. Privacy Research and Best Practices: Summary of a Workshop for the Intelligence Community. Washington, DC: The National Academies Press. doi:10.17226/21879.

Applicability Overview

- 0% of CIS Safeguards apply
- Between 1% and 60% of CIS Safeguards apply
- More than 60% of CIS Safeguards apply

Control	CIS Control Title	Applicability
1	Inventory and Control of Enterprise Assets	●
2	Inventory and Control of Software Assets	●
3	Data Protection	●
4	Secure Configuration of Enterprise Assets and Software	●
5	Account Management	●
6	Access Control Management	●
7	Continuous Vulnerability Management	●
8	Audit Log Management	●
9	Email and Web Browser Protections	●
10	Malware Defenses	●
11	Data Recovery	●
12	Network Infrastructure Management	●
13	Network Monitoring and Defense	●
14	Security Awareness and Skills Training	●
15	Service Provider Management	●
16	Application Software Security	●
17	Incident Response Management	●
18	Penetration Testing	●

CONTROL 01

Inventory and Control of Enterprise Assets

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.

Privacy Applicability

This CIS Control is applicable to the creation and maintenance of device inventories. Privacy principles should be incorporated into the device inventory process, from both a technological and a procedural standpoint. Many of the Safeguards within this Control are applicable to privacy.

Privacy Implications

- Knowledge about a device, where it is located, who is using it, and how they are using it, could provide information about an individual ("personal data"). Further, many enterprises use an individual's name or identifier, which explicitly links the device to the individual. Accordingly, inventories of enterprise assets should be handled as though they contain personal data. Note that this can occur with laptops, IoT, and mobile devices. At some point, it is possible for monitoring and tracking software to cross a line and negatively affect employee safety and privacy, essentially becoming employee "surveillanceware".
- It is common for enterprises to provision device models to employees based on their role within the enterprise. For instance, developers may be provisioned with more powerful laptops than general staff, or executives may receive tablets. Knowledge of this information could allow inference of the user's role in the enterprise and potentially associated characteristics such as likely salary range.
- With some mobile device deployment scenarios, such as Bring Your Own Device (BYOD) or Corporately Owned, Personally Enabled (COPE) mobile devices, device management platforms might track location of that device at any given time, which could expose the whereabouts of a user. Some device management platforms may also track device usage, and even the contents, which is likely to involve personal data.

Data Collection

Common data types collected for this CIS Control will include information about the device, such as model, owner, IP, and device name. Device name may include usernames or other user information. Identifying information (i.e., personal data) about the user is commonly stored in the device inventory, such as first name, last name, employee role, and potentially contact information such as phone number and email address. Information collected from mobile devices could include detailed information about the mobile device to include phone number and device identifiers.

Data Storage

Device inventory information may be stored in a Microsoft Excel spreadsheet located on a system administrator's system. The inventory may also be hosted within a database stored onsite within the enterprise network. It is quite common to use an application to assist with the creation and maintenance of a device inventory. That information may be stored locally but may also be stored in a cloud-based system outside of the enterprise's control. The external service provider may have access to all data inventory information, making the service provider's privacy policies relevant to know before usage. Any hot sites or other organizations/ hardware providing data redundancy may also store this data and user information.

Additional Discussion

Technical staff should work with the privacy officer or legal counsel to identify what requirements are needed for privacy protection in regard to this CIS Control. Privacy preserving hostnames are encouraged, especially for devices expected to operate outside the enterprise network (e.g., phones, travel laptops). Device inventories should be protected from unauthorized access and exposure via other relevant CIS Controls and Safeguards since they contain personal data and can be used to attack an enterprise, its employees, contractors, and service providers.

Automated inventory systems should be configured to collect only the information required by the enterprise for their inventory, and to delete obsolete information in a timely fashion. Automated inventory systems should also be manually audited to confirm data is being collected, maintained, and deleted as intended. This may require additional time and configuration. Documentation should explicitly reflect privacy decisions and associated rationales, and mitigations in place for hardware inventory creation and maintenance.

Fair Information Practice Principles

- **The Collection Limitation Principle.** IT should only collect the required data from devices when creating and maintaining an inventory. IT should carefully consider whether data is actually required to securely maintain and manage an inventory.
- **The Data Quality Principle.** Unnecessary data should not be collected or maintained within an enterprise asset inventory. Data should be updated on a regular basis and used only for data inventory purposes. Obsolete data should be deleted in a timely fashion.
- **The Purpose Specification Principle.** Employees should understand what personal data will be kept within the enterprise asset inventory, and how it will be used.
- **The Use Limitation Principle.** Personal data stored within enterprise asset inventories should not be shared or used for other purposes without explicit employee permission. Such other purposes should be necessary and reasonable.
- **The Security Safeguards Principle.** The CIS Controls can be leveraged to enable this principle, such as Control 3: Data Protection.
- **The Openness Principle.** Employees should understand what external systems may contain personal data and why.
- **The Individual Participation Principle.** Employees should have the ability to reasonably request to see what data is held about them in the inventory.
- **The Accountability Principle.** This principle must be discussed with the service provider before selection and usage.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should understand what personal data will be kept within the enterprise asset inventory, and how it will be used. A lawful basis is needed for collecting personal data within the enterprise asset inventory.
- **Purpose limitation.** Users should be informed in writing about your purpose for collecting personal data in the enterprise asset inventory from the outset of collecting it. Personal data kept within the enterprise asset inventory should only be used for inventory purposes. This may conflict with the need to leverage asset inventory data for secure baselines and vulnerability management. This may only apply to personally owned devices. Enterprise-owned devices may not be subject to this principle.
    - **Data minimization.** Unnecessary inventory data should not be collected or maintained within an enterprise asset inventory. The data that is collected for the hardware inventory must be specifically used for the hardware inventory and nothing else.
    - **Accuracy of data.** Data should be updated on a regular basis where necessary and used only for data inventory purposes. Written processes should be documented for how the enterprise asset inventory is maintained and how incorrect data is corrected.
    - **Storage limitation.** Inventory data that can identify an individual should only be stored for as long as needed. Obsolete data should be deleted without delay.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Control 3: Data Protection. Enterprise asset inventory data should be protected from unauthorized access, modification, and disclosure.

Control 1 Privacy Applicability Table

CIS Control 01: Inventory and Control of Enterprise Assets				Applicability Included?
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Justification and Privacy Considerations
1.1	Devices	Identify	**Establish and Maintain Detailed Enterprise Asset Inventory** Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, 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.	**Yes** The information collected within asset inventories likely contains, or is directly connected to, information systems containing PII and other personal data. Make sure your enterprise has, and implements, a data handling policy for the inventory that applies the principles (above).
1.2	Devices	Respond	**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.	**Yes** Identifying and addressing unauthorized assets may intentionally or unintentionally involve the collection of personal data (e.g., the names of commonly used wireless fidelity (Wi-Fi) server set identifiers (SSIDs) used by a mobile device, which could contain individuals' names such as Alice and Bob or the name of a medical provider or other place the individual had previously visited).

CIS Control 01: Inventory and Control of Enterprise Assets				Applicability Included?
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Justification and Privacy Considerations
1.3	Devices	Detect	**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.	**Yes** Using automated tools to interrogate devices can obtain information that the enterprise could use to link devices to individuals. When interrogated, devices may offer identifying information in response.
1.4	Devices	Identify	**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.	**Yes** DHCP logs contain sensitive information because they map device identifiers to an IP address, so it's critical that an enterprise limit who has access, carefully protect the data, and have a data retention policy that limits the time it holds this data.
1.5	Devices	Detect	**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.	**Yes** Passive discovery may involve the collection and use of device identifiers that are unique (e.g., hostnames, media access control (MAC) addresses, and IP addresses). The enterprise likely has the ability to link those identifiers to individual users. When these identifiers are combined with other data about those users, the resulting information may be personal data. Even the identifiers, when linked or able to be linked to an individual, may be considered personal data.

CONTROL 02

Inventory and Control of Software Assets

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.

Privacy Applicability

This CIS Control is applicable to the development and maintenance of software inventories. Privacy principles should be incorporated into the software inventory process, from both a technological and a procedural standpoint. Multiple Safeguards were not included for privacy.

Privacy Implications

- Software inventories list authorized software (and versions) installed on enterprise approved devices. These software assets are directly tied to specific individuals and can collect and manipulate personal data about specific users.
- Certain software assets will contain information about employees, such as health information from sponsored wellness applications, financial information from accounting and payroll software, and personal information from human resource management software.
- Software on personal BYOD-enabled mobile devices may be able to access or request personal information related to lifestyle, health tracking, or personal finances. When users are using personal devices for work, this becomes more acute, as certain applications could indicate lifestyles that might be used to discriminate against specific employees. At some point, it is possible for monitoring and tracking software to cross a line and negatively affect employee safety and privacy, essentially becoming employee "surveillanceware".

Data Collection

Common forms of data collected for this CIS Control will include information about the device to include model, owner, IP, and device name. Device name may include usernames or other user information such as first name, last name, employee role, and potentially contact information (e.g., phone number, email address). Information about other software installed on the system is likely to be available.

Data Storage

This information may be stored in a Microsoft Excel spreadsheet located on a system administrator's system or hosted within a database stored onsite within the enterprise network. It is common to use an application to assist with software inventory. That information may be stored locally but may also be stored in a cloud-based system outside of the enterprise's control. The service provider may have access to all data inventory information. Any hot sites or other organizations providing data redundancy may also store this inventory and user information.

Additional Discussion

In the software inventory, effort should be made to identify software likely to contain personal or confidential information. Apply appropriate protections to the inventory and to sensitive software. Enterprises should have a privacy policy that lets users know these characteristics and what could be derived from the devices they own. Furthermore, automated systems should be configured appropriately to only collect necessary information, and documentation should explicitly reflect the privacy decisions and mitigations in place. IT should be made aware of privacy decisions within this process and follow approved documentation.

Fair Information Practice Principles

- **The Collection Limitation Principle.** IT should only collect the required data from software when creating and maintaining an inventory.
- **The Data Quality Principle.** Unnecessary data should not be maintained within a software inventory. Data should be updated on a regular basis and used only for data inventory purposes.
- **The Purpose Specification Principle.** Employees should understand what personal data will be kept within the software inventory, and how it will be used.
- **The Use Limitation Principle.** Personal data stored within software inventories should not be used for purposes other than those previously established, without explicit employee or customer permission.
- **The Security Safeguards Principle.** Technical staff should work with the corporate privacy officer, or legal counsel, to identify what requirements are needed for privacy data protection.
- **The Openness Principle.** Employees should understand what external systems may contain personal data.
- **The Individual Participation Principle.** Employees should have the ability to reasonably request to see what data is held about them in the inventory.
- **The Accountability Principle.** This principle must be discussed with the service provider before selection and usage.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should understand what personal data will be kept within the software asset inventory, and how it will be used. A lawful basis is needed for collecting personal data, in this case, what software would be on personal devices, within the software inventory.
- **Purpose limitation.** Users should be informed in writing about your purpose for collecting personal data in the software asset inventory from the outset of collecting it. Personal data kept within the software inventory should only be used for inventory purposes. This may conflict with the need to leverage software inventory data for secure baselines and vulnerability management. This may only apply to personally owned devices. Enterprise-owned devices may not be subject to this principle.
- **Data minimization.** Unnecessary software inventory data should not be collected or maintained within an enterprise asset inventory. The data that is collected for the software inventory must be specifically used for the software inventory and nothing else.
- **Accuracy of data.** Inventory data should be updated on a regular basis where necessary and used only for data inventory purposes. Written processes should be documented for how the software inventory is maintained and how incorrect data is corrected.
- **Storage limitation.** Inventory data that can identify an individual should only be stored for as long as needed. Obsolete data should be deleted without delay.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Control 3: Data Protection. Software inventory data should be protected from unauthorized access, modification, and disclosure.

Control 2 Privacy Applicability Table

CIS Control 02: Inventory and Control of Software Assets				
Safeguard	**Asset Type**	**Security Function**	**Control Title/ Description**	**Applicability Included? Applicability Justification and Privacy Considerations**
2.1	Applications	Identify	**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.	**Yes** The information collected within asset inventories likely contains, or is directly connected to, information systems containing PII and other personal data.
2.2	Applications	Identify	**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.	**No** Ensuring software assets are supported does not present privacy impacts.
2.3	Applications	Respond	**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.	**No** Removing unauthorized applications does not present privacy impacts, although it may cause the deletion of an employee's personal data (e.g., photos in a photo sharing app). Deletion of an individual's personal data could be a privacy impact in some circumstances. But, the enterprise may state that the employee was not authorized to create, collect, receive, share, or store that data on the device.
2.4	Applications	Detect	**Utilize Automated Software Inventory Tools** Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.	**Yes** Using automated tools to actively identify installed applications will likely provide personal data to the employer, especially on mobile platforms. This may include information about apps related to lifestyle, health tracking, or personal finances.
2.5	Applications	Protect	**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.	**Yes** Allowlisting software on personal mobile devices may be privacy-invasive based on the mobile operating system and specific implementation.
2.6	Applications	Protect	**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.	**No** This specific type of allowlisting does not present privacy impacts.
2.7	Applications	Protect	**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.	**No** This specific type of allowlisting does not present privacy impacts.

CONTROL 03

Data Protection

OVERVIEW

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

Privacy Applicability

Data Protection is a CIS Control that can help to protect a myriad of information types throughout an enterprise network, including PII and other personal data. Without the Safeguards listed here, much of the personal and customer information that enterprises keep would be at risk of unauthorized exposure. Yet, as stated in this guide's Scope, keeping information safe from unauthorized disclosure is not the only consideration for being applicable to privacy. If it were the only consideration, then all of the Safeguards within the CIS Controls would be applicable. As such, only some of the Safeguards are listed as applicable.

Privacy Implications

- Failure to implement many of the Safeguards within this CIS Control would likely be insufficient to protect PII and other personal data.
- Portable devices and media likely store PII and other personal data. Although addressing these form factors can be difficult, it is worth the extra effort and expenditure.
- Implementing many of the Safeguards within this Control can protect PII and other personal data. Yet, these same systems may require privileged roles and access to function as intended. Understanding the actions software is taking in the background and what information is being collected is a worthwhile activity.

Data Collection

Types of information should be labeled according to the data scheme established in Safeguard 3.7 – Establish and Maintain a Data Classification Scheme. This does not necessarily need to be performed in an automated fashion via software, but IT administrators and Privacy Officers should have a general knowledge of the types of data collected. IT employees should know how to identify and report instances of newly discovered personal data.

Safeguard 3.13 – Deploy a Data Loss Prevention (DLP) Solution can be leveraged in an automated fashion to identify collected PII and other personal data in the enterprise. DLP usage may reveal unknown PII and personal data, and should be monitored regularly. Access to sensitive data should be logged in accordance with Safeguard 3.14 – Log Sensitive Data Access. This ensures that, upon review of logs, it can be determined that only authorized individuals were able to access personal data. This likely cannot be accomplished on mobile devices.

Data Storage

Data inventories should be protected with Safeguards from this Control. Any data stored in cloud systems should also be protected, and personal data stored there should be explicitly understood and approved. Please see the CIS Controls Cloud Companion Guide for how to secure cloud-based systems.

Disposal of stored personal data (Safeguard 3.5) should be accomplished in a secure manner in consultation with the enterprise's information security office or existing policy. This should be performed for all physical paper, digital media, and IoT and mobile platforms.

Additional Discussion

There are few direct privacy implications relating to CIS Control 3, as most of the Safeguards actively enhance privacy by preventing information from unauthorized disclosure. With that said, privacy implications exist for some Safeguards as mentioned above. A data management process, to include a data inventory classification scheme, could be interpreted in a manner to enhance privacy. These Safeguards can also be used to help understand the types of personal and customer data stored within the enterprise (e.g., PII, proprietary), and data classifications can then be leveraged to identify necessary data protection methods that assist in privacy protections.

Implement auditing of regulatory and third-party agreement requirements to verify the location and appropriate protection of all privacy data. As previously noted, many of the Safeguards in this Control play a pivotal role in protection of private information, such as the use of cryptography. When in doubt, enterprises are encouraged to use the Control 3 Safeguards because they protect personal data. Additionally, if there is a breach, it may be possible to prove lack of sufficient controls to protect data. Incorrect implementation of encryption, use of weak encryption algorithms, or insecure management of encryption keys all create a situation rife for a data breach.

Fair Information Practice Principles

- **The Collection Limitation Principle.** Personal data generally should not be collected as part of this Control with the exception of data access logs and Data Loss Prevention (DLP) systems.
- **The Data Quality Principle.** Any collected data should be relevant to the reason it was collected. For instance, the DLP should not be collecting data it is not meant to collect.
- **The Purpose Specification Principle.** Employees should understand why certain systems such as DLP are collecting their data.
- **The Use Limitation Principle.** DLP or access log data should not be shared unless consent is provided.
- **The Security Safeguards Principle.** Control 3, and the CIS Controls in general, can assist in protecting PII and other personal data.
- **The Openness Principle.** People who have their data collected and logged should understand what external systems may contain personal data.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be kept as a result of the implementation of this Control. A lawful basis is needed for collecting personal data, in this case, what software would be on personal devices, within the software inventory.
- **Purpose limitation.** Users should be informed in writing about your purpose for collecting personal data from the outset of collecting it.
- **Data minimization.** Unnecessary personal and customer data should not be collected or maintained unless it is specifically needed. The data that is collected must be specifically used for its original intended purpose.

- **Accuracy of data.** All personal and customer data should be updated on a regular basis where necessary and used only for data management purposes. This includes DLP and log data. Written processes should be documented for how this data is maintained and how incorrect data is corrected.
- **Storage limitation.** Personal, customer, DLP, and log data that can help identify an individual should only be stored for as long as needed. Obsolete data should be deleted without delay.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Control 3: Data Protection. Software inventory data should be protected from unauthorized access, modification, and disclosure.

Control 3 Privacy Applicability Table

CIS Control 03: Data Protection				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
3.1	Data	Identify	**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.	**Yes** This can be leveraged to manage PII and other types of private information.
3.2	Data	Identify	**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.	**Yes** This can be leveraged to manage PII and other types of private information.
3.3	Data	Protect	**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.	**Yes** Only certain users and roles should be provided access to certain types of protected and private information.
3.4	Data	Protect	**Enforce Data Retention** Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	**Yes** The privacy implications associated with retained data should be analyzed and understood.
3.5	Data	Protect	**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.	**Yes** All enterprise data should be securely disposed of, especially if private or customer information is included.
3.6	Devices	Protect	**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.	**Yes** This helps protect stored information that is private.

CIS Control 03: Data Protection

Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
3.7	Data	Identify	**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.	**Yes** This can be leveraged to manage PII and other types of private information.
3.8	Data	Identify	**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.	**Yes** This can ensure an enterprise knows where personal data is likely to be sent and how it is likely to be protected.
3.9	Data	Protect	**Encrypt Data on Removable Media** Encrypt data on removable media.	**Yes** This helps protect stored information in transit that is private.
3.10	Data	Protect	**Encrypt Sensitive Data in Transit** Encrypt sensitive data in transit. Example implementations can include, Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).	**Yes** This helps protect stored information that is private.
3.11	Data	Protect	**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.	**Yes** This helps protect stored information that is private.
3.12	Network	Protect	**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.	**Yes** Personal data should only be stored in approved locations and on appropriate systems. Access should be appropriately restricted.
3.13	Data	Protect	**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.	**Yes** This can be helpful to identify PII and other personal data stored within the enterprise or leaving in an unauthorized manner.
3.14	Data	Detect	**Log Sensitive Data Access** Log sensitive data access, including modification and disposal.	**Yes** Only approved users and roles should access private information, and this can help create an audit trail to examine after the fact of a breach. Log data may also be useful in identifying if a breach occurred.

CONTROL 04

Secure Configuration of Enterprise Assets and Software

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).

Privacy Applicability

Secure configurations for hardware and software assets can help enable privacy for employees by preventing data breaches and account takeovers. Certain configuration settings in popular products can be viewed as outright vulnerabilities, whereas other settings may weaken a system or software and make it more susceptible to a successful attack. With that said, a majority of the Safeguards within this Control can have a privacy impact when implemented within an enterprise.

Privacy Implications

- Certain configurations of hardware and software can be viewed as negatively affecting the privacy of employees. Therefore, a privacy review of configuration settings by knowledgeable parties is necessary to ensure that certain products do not intentionally or unintentionally store or transmit private employee data.
- Configuring certain assets appropriately may cause data to be collected, such as traffic logs or data access logs. Because this information can be sensitive, IT must understand the settings they are enabling so that this information isn't left in an unprotected state.
- Network appliances and applications such as Domain Name System (DNS) and firewalls will granularly track users by functioning as intended. How these appliances and applications function must be understood by IT, so that their data can be regularly maintained and protected.

Data Collection

Configurations for enterprise assets and software should be enabled in a manner that refrains from collecting personal data from employees as much as is practical. This means that systems with options to host or send data to other service providers should not be configured to do so.

Data Storage

To the extent practical, systems owned and operated by external service providers should not be configured to store personal data outside the enterprise. As few parties as possible, if any, should have access to the employee information and only for legitimate purposes.

Additional Discussion

Many of the Safeguards in this Control help to provide basic protections against common forms of unauthorized access, such as via the use of a lock screen password in Safeguard 4.3 – Configure Automatic Session Locking on Enterprise Assets. Proper configuration for all enterprise assets should be accomplished via a secure configuration process for both traditional systems and network assets (Safeguards 4.1, 4.2). This should include proper configuration of server firewalls and on-device host-based firewall software (Safeguards 4.4, 4.5).

Configuration of mobile devices to support privacy can be difficult to balance. While the enterprise needs the ability to securely manage and govern access to enterprise data on a mobile device, these devices also contain extremely personal and private information. Regardless of device ownership, effort should be made to minimize enterprise access to personal employee information. This can be configured via Enterprise Mobility Management (EMM) tools which help enable Safeguards 4.11 and 4.12. These tools do not necessarily need control of the entire device but can manage a single application that contains all enterprise data, which allows for separate work environments (4.12) and easy deletion of data as needed (4.11). Please refer to the CIS Controls Mobile Companion Guide for additional discussion regarding mobile security.

Fair Information Practice Principles

- **The Collection Limitation Principle.** Employees in the U.S. are typically notified that their activities are being tracked by their employers in the U.S. via various IT policies such as acceptable use. This should be done to comply with this principle.
- **The Data Quality Principle.** Any collected data should be relevant to the reason it was collected, in this case, network appliances protecting the network and other software and systems protecting the network.
- **The Purpose Specification Principle.** Employees should understand why network-based appliances are collecting their data.
- **The Use Limitation Principle.** Network data about user activities on the internet should not be shared unless consent is provided. This includes providing network data to other service providers.
- **The Security Safeguards Principle.** Care should be taken to secure any stored network data, which likely includes PII and other personal data.
- **The Openness Principle.** People who have their data collected and logged should understand what external systems may contain their personal data.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be kept as a result of the implementation of this Control. A lawful basis is needed for collecting personal data, in this case, what software would be on personal devices, within the software inventory.
- **Purpose limitation.** Users should be informed in writing about your purpose for collecting personal data from the outset of collecting.
- **Data minimization.** Unnecessary personal and customer data should not be collected or maintained unless it is specifically needed. The data that is collected must be specifically used for its original intended purpose. Employees should understand why certain systems such as DLP are collecting their data.
- **Accuracy of data.** All personal and customer data should be updated on a regular basis where necessary and used only for specific purposes. Written processes should be documented for how this data is maintained and how incorrect data is corrected.
- **Storage limitation.** Personal, customer, and log data (e.g., traffic, application, DNS) that can help identify an individual should only be stored for as long as needed. Obsolete data should be deleted without delay.

- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle. Much of the personal and customer information that enterprises store can be prevented from unauthorized exposure if Safeguards within this Control are put into place. In addition to this principle of GDPR, many of the Safeguards within this Control can help fulfill the provisions of Article 32 of GDPR titled Security of processing. Article 32 1(a) states that, in specific circumstances, data processors shall protect personal data, to include the use of pseudonymized data, via encryption. Safeguards 3.6, 3.9, 3.10, and 3.11 can help to accomplish this task.

Control 4 Privacy Applicability Table

CIS Control 04: Secure Configuration of Enterprise Assets and Software				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
4.1	Applications	Protect	**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.	**Yes** Secure configuration processes should take privacy into account when deciding upon configurations. This should include what data is generated, and where it is stored. It should also include who can access, collect, and store PII and other personal data.
4.2	Network	Protect	**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.	**Yes** Privacy should be considered when deciding upon configurations. At the very least, users connected to enterprise networks should be guarded from low-effort passive enumeration sweeps.
4.3	Users	Protect	**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 two minutes.	**No** This helps prevent naive attempts to access unauthorized personal data, but there are no privacy impacts.
4.4	Devices	Protect	**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.	**Yes** While this Safeguard can help prevent a data breach, which would be an unauthorized exposure of PII and other personal data, the privacy impact is the system and software reading or sniffing user traffic.
4.5	Devices	Protect	**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.	**Yes** While this Safeguard can help prevent a data breach, which would be an unauthorized exposure of PII and other personal data, the privacy impact is the system and software watching user activities.
4.6	Network	Protect	**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 (HTTPS). Do not use insecure management protocols, such as Telnet and HTTP, unless operationally essential.	**Yes** System administrators will at times have to access PII and other personal data. Using secure protocols and access control to do so prevents eavesdropping and other attacks over the wire. System administrators should be trained on acceptable activities and how to avoid violations of user privacy when acting as administrator.

CIS Control 04: Secure Configuration of Enterprise Assets and Software

Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
4.7	Users	Protect	**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.	**Yes** Certain accounts on systems will be given additional privileges and may be able to access personal data. Access to these accounts needs to be properly managed, with users of those accounts properly trained on how to avoid violations of user privacy.
4.8	Devices	Protect	**Uninstall or Disable Unnecessary Services on Enterprise Assets and Applications** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.	**Yes** Unnecessary services can be a vector for unauthorized access and should be disabled. Unnecessary services may act as spyware and collect user information. However, some services that might be considered unnecessary by an enterprise could actually improve security and privacy, e.g., if an enterprise chooses not to supply a virtual private network (VPN), but the user is using a reputable, trusted service, or the user has included an ad-blocking, anti-tracking extension in their browser. Uninstalling or disabling services, especially without notice to the user, could cause the loss of personal data stored in those services to that user. However, the enterprise would argue those services were unauthorized in any event.
4.9	Devices	Protect	**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.	**Yes** Using an untrusted DNS server could trick users into providing personal data to malicious parties. It is possible that a DNS provider may sell/share the DNS traffic with advertisers or others, which would have a privacy impact.
4.10	Devices	Respond	**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.	**No** This helps prevent naive attempts to access unauthorized personal data on the devices. It also helps prevent more sophisticated cracking attempts. There is no privacy impact.
4.11	Devices	Protect	**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.	**Yes** This Safeguard can help remove personal data if a device is lost or stolen or the holder of the device is no longer authorized to access the data.
4.12	Devices	Protect	**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.	**Yes** Separate workspaces help enterprises easily access, manage, and delete only enterprise information. They can also assist with private usage of a mobile device by only providing enterprise access to the workspace on the phone managed by the employer.

CONTROL 05

Account Management

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.

Privacy Applicability

Authentication is a large complex topic that includes creating identities, binding credentials, assigning privileges, and generally managing the lifecycle of accounts. This Control focuses on managing various aspects of the authentication process. Account management is applicable to all applications, devices, and services used by the enterprise. Every employee within the enterprise will need an account to access applications, devices, and internal or external service providers in order to use them. A majority of the Safeguards in this Control will have some amount of privacy impact.

Privacy Implications

- Personal data can be leaked through the creation, usage, and disclosure of credentials. Users should refrain from putting personal data into passwords and other credentials, including responses to account security questions. At times, this information may not be stored securely, and if stolen or leaked could be used to break into other accounts.
- When malicious actors hack an enterprise, they often release passwords and other credentials to the public. Other account information may also be included within any leaked databases, which can include usernames and/or email addresses. Service provider accounts may also be affected.

Data Collection

Usernames, identifiers (e.g., email addresses), and credentials such as passwords and cryptographic information will be collected by internal enterprise applications and services, alongside third-party service providers that require authentication. Biometric information is another area of concern. During enrollment, these systems may also take biometric samples such as iris, facial, or fingerprint scans, which are then used to create biometric templates. These templates contain uniquely personal information, and if designed poorly can be used to reverse-engineer the biometrics of the individual or characteristics of their biometrics. It is generally unknown to an end-user what data is collected, how it is stored, whether it will be kept secure, and if it will be deleted when no longer needed.

Data Storage

Secure storage of enterprise account information and other data pertaining to authentication can be solved by implementation of several CIS Controls. Systems that store account information need to remain up-to-date on patches and ensure secure methods of storage are applied accordingly, including use of hashed and salted passwords alongside the use of encryption where applicable. All enterprises should understand the security practices being used to protect information before using any third-party service.

Additional Discussion

Using authentication platforms that allow for a single identity and set of credentials to access multiple services is a security best practice. However, these federated-identity or Single Sign-On (SSO) systems do have access to all authentication information within an enterprise, which could be misused, and may not be the best tools from a privacy perspective. The privacy policies and practices of SSO services should be carefully scrutinized before they are engaged.

Fair Information Practice Principles

- **The Collection Limitation Principle.** When creating an account, IT should refrain from obtaining more personal data than is needed.
- **The Data Quality Principle.** Any collected personal data should be used only for access or verifying access to enterprise systems.
- **The Purpose Specification Principle.** Employees should be informed why their personal information is being collected and how it will be used.
- **The Use Limitation Principle.** Employees should be informed if this information will be used to create accounts on future systems owned by third-party service providers or to allow third-parties access to their data.
- **The Security Safeguards Principle.** Care should be taken to secure any stored and transmitted credential data, which likely includes PII and other personal data.
- **The Openness Principle.** People who have their data collected for account creation and/or account management (e.g., access) should understand what external systems may contain or have access to their personal data and why.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs. Enterprises are encouraged to use SSO providers that support MFA and do not share user data with other third-party organizations.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be collected, retained, and shared as a result of account creation and maintenance. A lawful basis is needed for collecting and sharing personal data, in this case, potentially name, address, email, telephone, and other information.
- **Purpose limitation.** Users, to include employees and customers, should be informed in writing about your purpose for collecting personal data from the outset of collecting it. Personal data kept within the identity management platform, domain controller, or similar platform should only be used for account management. This may conflict with the need to integrate the domain controller with third-party software and platform. Employees should be informed if this information will be used to create accounts on future systems owned by third-party service providers.
- **Data minimization.** During the account creation process for a new user, the IT staff should refrain from obtaining more information than is needed. All data collected during the account creation process should be specifically used for account creation and maintenance. Account data should be deleted when no longer needed.
- **Accuracy of data.** All user and customer data associated with accounts should be updated on a regular basis where necessary and used only for account management. Written processes should be documented for how this data is maintained and how incorrect data is corrected or deleted. These processes should also include how customers can access and modify their own data.

- **Storage limitation.** Employee and customer data that can help identify an individual should only be stored for as long as needed. Obsolete data should be deleted without delay. Much of the information associated with employee accounts will need to be kept indefinitely.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Control 3: Data Protection. Employee and customer account data should be protected from unauthorized access, modification, and disclosure.

Control 5 Privacy Applicability Table

CIS Control 05: Account Management				
Safeguard	**Asset Type**	**Security Function**	**Control Title/ Description**	**Applicability Included? Applicability Justification and Privacy Considerations**
5.1	Users	Identify	**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.	**Yes** Account inventories are likely to contain personal data, which may include PII and personal data. This information needs to be appropriately protected. A process should be written to best follow this Safeguard.
5.2	Users	Protect	**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.	**Yes** Users should be instructed to refrain from using personal information within passwords. Additionally, the system should warn users against the usage of the most common passwords.
5.3	Users	Respond	**Disable Dormant Accounts** Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	**No** Preventing dormant accounts from being used helps prevent unintended disclosure of personal data that could be accessed via those accounts.
5.4	Users	Protect	**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.	**Yes** Although this is a best practice in and of itself, it can help an enterprise protect personal data since administrator accounts are often high value targets for malicious actors and generally have greater access to personal data on the enterprise's network. Restricting privileges also restricts administrative managing of PII and other information unless needed.
5.5	Users	Identify	**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 all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	**Yes** Depending on how service account inventories are developed, they may contain PII and personal data. This information needs to be appropriately protected. A process should be written to best follow this Safeguard.
5.6	Users	Protect	**Centralize Account Management** Centralize account management through a directory or identity service.	**Yes** Centralized account management can significantly benefit an enterprise from a security perspective, but the external enterprise providing federation services may have access to personal data and be able to correlate a user's activities and behavior across multiple services.

CONTROL 06

Access Management Control

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.

Privacy Applicability

The Access Management Control is meant to manage large portions of the authentication and authorization process, ranging from how a user accesses a device through revoking access credentials and privileges. Thorough implementations of CIS Control 5 and Control 6 involve written policies addressing these areas before devices and account access to other services are provided to users. While the impact of the Safeguards within this Control affects overall security in a major way, the privacy impact is generally minor.

Privacy Implications

- PII and other personal data are often stored within authentication and authorization systems. These systems need to be set up in a privacy preserving manner to the extent practical. Generally, automated access management is preferred as it helps to prevent any accidental private and sensitive information exposures by people.
- The revocation of rights should preferably be performed in an automated manner to prevent a human from viewing personal information stored with accounts. To that extent, there may be some forms of PII and Protected Health Information (PHI) that system administrators do not need privileges to access. Failure to control access, even from administrators, could be a compliance requirement or could lead to unauthorized access and disclosure.
- Logs relating to authentication and authorization systems in general may record private action. For instance, some remote access and multifactor authentication mechanisms log the geolocation of users when they connect. Other authentication events will trigger logs such as time of access, time of authentication attempt, and resources accessed. Although these logs are not necessarily negative, they can be used to thwart privacy. Due to this and other factors, it is best practice to regularly audit and verify who has access to authentication and authorization data, and to only keep such data for as long as it is needed.

Data Collection

The information systems that help administrators manage rights and privileges within their enterprise may have collected personal data when enrolling users. Administrators and third-party service providers will generally have access to this data. This is also true for the authentication systems used for remote users. Geolocation information and data from device fingerprinting is likely to be collected by both parties.

Data Storage

The information systems that help administrators manage rights and privileges must store the information they collected. Access management third-party service providers will generally have access to this information.

Additional Discussion

When considering the assignment of privileges to users and their credentials, this Control is concerned with protection of the privileges themselves. Secure authentication enables privacy on a network, as the user is able to access enterprise sources without eavesdropping. Rights and privileges are not always provided; sometimes they must be removed.

Fair Information Practice Principles

- **The Collection Limitation Principle.** When granting access to new resources, IT should refrain from obtaining more information from an employee than is needed.
- **The Data Quality Principle.** Any collected personal data should be used only for access to enterprise systems.
- **The Purpose Specification Principle.** Employees should be informed why their personal data and privileges are being collected and how they will be used.
- **The Use Limitation Principle.** Employees should be informed if this data will be used to create accounts on future systems owned by third-party service providers or to allow third-parties to access their data.
- **The Security Safeguards Principle.** Care should be taken to secure any stored and transmitted credential data, which likely includes PII and other personal data.
- **The Openness Principle.** People who have their data collected for account creation should understand what external systems may contain their personal data and why.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be collected, used, or retained as a result of account creation and maintenance. A lawful basis is needed for collecting personal data.
- **Purpose limitation.** Access privileges kept within the identity management platform or domain controller or similar platform should only be used for account management. This may conflict with the need to integrate the domain controller with third-party software and platform. Employees should be informed if this information will be used to create accounts on future systems owned by third-party service providers.
- **Data minimization.** All information collected during the account creation process and through regular usage should be meant for a pre-specified purpose.
- **Accuracy of data.** All user and customer information associated with accounts, privileges, and access should be updated on a regular basis where necessary and used only for account management. Written processes should be documented for how this data is maintained and how incorrect data is corrected.
- **Storage limitation.** Employee and customer data that can help identify an individual should only be stored for as long as needed. Obsolete data should be deleted without delay. Much of the access control lists and privileges associated with employee accounts may need to be stored for extended periods of time for incident response and auditing purposes.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Control 3: Data Protection. Employee and customer account data, to include lists of access and privileges, should be protected from unauthorized access, modification, and disclosure.

Control 6 Privacy Applicability Table

CIS Control 06: Access Management Control				
Safeguard	**Asset Type**	**Security Function**	**Control Title/ Description**	**Applicability Included? Applicability Justification and Privacy Considerations**
6.1	Users	Protect	**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.	**Yes** Privacy of employee information should be taken into account when establishing this process. An automated process is preferred as a person does not need to view PII and other personal data. Automated processes are preferred because these can often be implemented with the appropriate privacy protections.
6.2	Users	Protect	**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.	**Yes** The revocation of rights should preferably be performed in an automated manner to prevent a human from viewing this information.
6.3	Users	Protect	**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.	**Yes** Some remote access and multifactor authentication mechanisms log the geolocation of users when they connect, which is personal data. They may also collect other personal data through device fingerprinting or other means to verify the identity of the user.
6.4	Users	Protect	**Require MFA for Remote Network Access** Require MFA for remote network access.	**Yes** Some remote access and multifactor authentication mechanisms log the geolocation of users when they connect, which is personal data. They may also collect other personal data through device fingerprinting or other means to verify the identity of the user.
6.5	Users	Protect	**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.	**Yes** Although a best practice, there are no major privacy concerns with the implementation of this Safeguard. Some remote access and multifactor authentication mechanisms log the geolocation of users when they connect or use insecure SMS, and may tracks users' access to services and across services (e.g., authentication apps).
6.6	Users	Identify	**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.	**Yes** Personal data is often stored within authentication and authorization systems. These systems need to be set up in a privacy preserving manner in as practical a manner as possible.
6.7	Users	Protect	**Centralize Access Control** Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.	**Yes** Centralized access control can significantly benefit an enterprise from a security perspective, but any external organization providing these services may have access to personal information.

CIS Control 06: Access Management Control				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
6.8	Data	Protect	**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 all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.	**No** There are no privacy impacts when using role-based access control, unless individual users are highlighted as roles within these systems or that information is otherwise available (e.g., can be inferred from the organizational chart or bios on the enterprise's website).

CONTROL 07

Continuous Vulnerability Management

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.

Privacy Applicability

This Control focuses on using software to monitor the vulnerabilities contained within software used by an enterprise. Applying the guidance from the CIS Controls for vulnerability management will contribute to situational awareness of vulnerabilities and taking proactive action for potential weaknesses in privacy supporting defensive mitigations. Control 7 does not contain a large number of Safeguards with a privacy impact. For instance, automated patch management and vulnerability remediation generally do not affect privacy or cause the exposure of sensitive data.

Privacy Implications

- Combining an enterprise's asset inventory with the tools and software ecosystem used for vulnerability scanning may share PII and other personal data with another enterprise. Asset inventories often have granular information about specific individuals, such as name, telephone number, email, and physical address. Personal information about assets and specific individuals assigned to them should not be provided to vulnerability management systems.
- Forcing updates on employee-owned devices without explicit agreement may be problematic. Privacy implications generally don't exist with remediating vulnerabilities for company-owned property.

Data Collection

To the extent practical, vulnerability management software should be configured to refrain from collecting identifying information about systems. Connecting inventories with vulnerability management systems is often best practice, but oversharing can have a privacy impact. This vulnerability management software will have access to all of this information without the consent of the individual.

Data Storage

To the extent practical, enterprises should host all data relating to this software on-premises, and not in a cloud platform owned and operated by a third-party service provider.

Additional Discussion

There may be regulatory requirements or third-party agreements for identifying and managing vulnerabilities to systems that store personal data. Some of these regulatory requirements may specifically call out the need for managing vulnerabilities in order to protect personal data from unauthorized disclosure. Enterprises should understand the privacy laws governing their county, state, region, and industry.

Fair Information Practice Principles

- **The Collection Limitation Principle.** If a vulnerability management suite does not require access to PII and other personal data stored within the software and hardware inventory to function, then the information should not be provided.
- **The Data Quality Principle.** Any collected data, either from the software inventory, or directly from the host, should be used solely for vulnerability management purposes.
- **The Purpose Specification Principle.** Employees should be informed why their personal information is being collected by vulnerability management agents, and how the information will be used.
- **The Use Limitation Principle.** Employees should be informed if this information will be transferred to other systems owned by third-party service providers.
- **The Security Safeguards Principle.** Care should be taken to secure any stored and transmitted vulnerability data, which likely includes PII and other personal data.
- **The Openness Principle.** People who have their data collected by vulnerability management systems should understand what external systems may contain their personal data and why.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision about their use of enterprise assets based on the type of personal data that will be in a vulnerability management platform. A lawful basis is needed for collecting personal data.
- **Purpose limitation.** Users should be informed in writing about your purpose for collecting personal data in the vulnerability management platform from the outset of collecting it. Personal data obtained for vulnerability management should only be used for this system and employees should be informed if their information will be transferred to other systems owned by third-party service providers. Enterprise-owned devices may not be subject to this principle.
- **Data minimization.** Nothing more than is necessary for vulnerability management should be collected. There will likely be significant overlap with the information collected for the enterprise asset and software inventories.
- **Accuracy of data.** User data in vulnerability management should be regularly checked for accuracy. Written processes should be documented for how user data in vulnerability management platforms is maintained and how incorrect data can be corrected or deleted.
- **Storage limitation.** User data should only be stored for as long as needed in a vulnerability management platform. Obsolete data should be deleted without delay.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Controls 3, 4, and 5. Vulnerability data should be protected from unauthorized access, modification, and disclosure and can be leveraged by an attacker to obtain unauthorized access to an enterprise's systems.

Control 7 Privacy Applicability Table

CIS Control 07: Continuous Vulnerability Management				
Safeguard	**Asset Type**	**Security Function**	**Control Title/ Description**	**Applicability Included? Applicability Justification and Privacy Considerations**
7.1	Applications	Protect	**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.	**Yes** Personal information about assets and specific individuals assigned to them should not be provided to vulnerability management systems. Personal data stored on enterprise assets should be taken into consideration.
7.2	Applications	Respond	**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.	**Yes** No potential for exposing sensitive information to unauthorized parties via this Safeguard. If the remediation process can result in deletion of user data, then there is a privacy concern.
7.3	Applications	Protect	**Perform Automated Operating System Patch Management** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	**No** Using automated patch management should not have an impact on privacy.
7.4	Applications	Protect	**Perform Automated Application Patch Management** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	**No** Using automated patch management should not have an impact on privacy.
7.5	Applications	Identify	**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.	**Yes** Assets on an internal network may have hostnames that expose information about an individual. If a vulnerability scanning tool is able to ascertain what applications are installed on a system this may be a privacy concern.
7.6	Applications	Identify	**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.	**Yes** Assets on an external network may have hostnames and often identifying features that may expose information about an individual. If a vulnerability scanning tool is able to ascertain what applications are installed on a system this may be a privacy concern.
7.7	Applications	Respond	**Remediate Detected Vulnerabilities** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.	**No** No privacy implications exist with remediating vulnerabilities for company-owned property.

CONTROL 08

Audit Log Management

OVERVIEW

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

Privacy Applicability

Firmware, software, systems, and services all generate audit logs. Logs help developers design and create products, while also helping IT staff to diagnose existing issues. These same logs also help create an audit trail to understand the actions that systems and users took while using the system. Control 8 includes all of these activities. Many of the Safeguards within this Control carry privacy implications, as logs may contain personal data.

Privacy Implications

- Logs may contain PII and other personal data such as usernames, roles, and other information collected by the software writing to a log file. In order to avoid this, an audit log management process that takes privacy into account should be defined (Safeguard 8.1).
- Many disparate systems create and store audit logs. It is important to understand what systems, software, libraries, and even network devices should have their logs collected and regularly analyzed.

Data Collection

Audit logs should only be collected by third-parties if explicitly agreed upon and with appropriate privacy protections. Workforce members should be trained to refuse third-party log collection, unless explicitly authorized by the enterprise, and ensure a log retention duration is decided upon and applied. Older log files should be archived and protected via cryptography and access control mechanisms to prevent a breach from accessing all of an enterprise's logs.

Data Storage

Log data should only be stored in secure locations with appropriate security controls. These are not secondary systems or storage locations; log data needs to be protected with regularly verified, defensive mitigations. This includes third-party service providers, with security controls generally known, and agreed upon in writing.

Additional Discussion

Administrators should work with the enterprise privacy officer, or legal department, to understand what potential PII is stored in logs and alerts. It is possible that personal data is logged or cached at the system or application level. Log data should be protected at the same level as the data itself, including appropriate retention limits. Finally, developers, both full-time employees and contractors, should be trained to avoid placing personal information within audit logs and alerts used to notify users.

Fair Information Practice Principles

- **The Collection Limitation Principle.** Enterprise systems should be configured to write as little PII and personal data to logs as possible.

- **The Data Quality Principle.** Any log data with personal information should only be used in business processes requiring logs, such as reviewing an audit trail or troubleshooting system failures.
- **The Purpose Specification Principle.** Employees should be informed what information may be stored in log files, and how the information will be used.
- **The Use Limitation Principle.** Employees should be informed if log information will be transferred to other systems owned by third-party service providers, such as a Security Information and Event Management (SIEM) that is not hosted on-premises.
- **The Security Safeguards Principle.** Care should be taken to secure any stored log data, which likely includes PII and other personal data.
- **The Openness Principle.** Employees with PII and other personal data collected by enterprise systems should understand what external systems may contain their personal data.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be stored in logs and subsequently collected by an enterprise. A lawful basis is needed for collecting logs containing personal data.
- **Purpose limitation.** Employees should be informed what information may be stored in log files, and how the information will be used, including transferring this data to a third-party for further analysis and correlation. Even enterprise-owned devices are subject to this principle under GDPR.
- **Data minimization.** Nothing more than is necessary should be written to log files and then subsequently collected or used by the enterprise.
- **Accuracy of data.** User data in logs should be checked for accuracy. Any storage locations of logs should also be verified to ensure they are storing the correct logs in the correct format. Written processes should be documented for how user data in logs is written and maintained.
- **Storage limitation.** User data should only be stored for as long as needed in a log platform. Obsolete data should be deleted without delay. Log files may need to be stored for a significant period of time for incident response, auditing, and troubleshooting purposes.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Controls 3 and 15. Log data should be protected from unauthorized access, modification, and disclosure and can be leveraged by an attacker to obtain unauthorized access to an enterprise's systems.

Control 8 Privacy Applicability Table

CIS Control 08: Audit Log Management				
Safeguard	**Asset Type**	**Security Function**	**Control Title/ Description**	**Applicability Included? Applicability Justification and Privacy Considerations**
8.1	Network	Protect	**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.	**Yes** Privacy should be a major consideration in the development of an audit log management process. This process should consider log rotation and the information that is collected within logs.
8.2	Network	Detect	**Collect Audit Logs** Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	**Yes** Personal devices should not have their logs collected and viewable by the enterprise unless needed and previously discussed.
8.3	Network	Protect	**Ensure Adequate Audit Log Storage** Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	**No** The size and location of audit log storage does not carry privacy considerations.
8.4	Network	Protect	**Standardize Time Synchronization** Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.	**No** No privacy implications exist for cross-organizational time synchronization.
8.5	Network	Detect	**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.	**Yes** Detailed audit logs may contain PII and other personal data. Whether this information should be collected in the first place should be considered, and best practices in privacy protection should be included.
8.6	Network	Detect	**Collect DNS Query Audit Logs** Collect DNS query audit logs on enterprise assets, where appropriate and supported.	**Yes** DNS query logs can easily be used to track users and the sites they have visited, even on authorized personal devices accessing the network. They should be treated as though they are personal data.
8.7	Network	Detect	**Collect URL Request Audit Logs** Collect URL request audit logs on enterprise assets, where appropriate and supported.	**Yes** Uniform Resource Locator (URL) request logs can easily be used to track users and can contain personal data, even on authorized personal devices accessing the network. They should be treated as though they are personal data.
8.8	Devices	Detect	**Collect Command-Line Audit Logs** Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.	**Yes** Command-line audit logs can be used to track how a user uses a system in a very granular manner. This can reveal information about the user, e.g., if they are using an accessibility device, their work patterns, etc.
8.9	Network	Detect	**Centralize Audit Logs** Centralize, to the extent possible, audit log collection, and retention across enterprise assets.	**Yes** The confluence of all audit logs can offer a very granular view into the activities of specific individuals and potentially their personal activities.

CIS Control 08: Audit Log Management				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
8.10	Network	Protect	**Retain Audit Logs** Retain audit logs across enterprise assets for a minimum of 90 days.	**Yes** Logs should only be actively stored online for specific lengths of time. Longer periods of time may exacerbate a data breach.
8.11	Network	Detect	**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.	**Yes** Processes should be developed for how to ensure privacy during audit log reviews. These processes should include incident response personnel with a particular interest towards third-party personnel. Training can help assist in this endeavor.
8.12	Data	Detect	**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.	**Yes** Authorized service providers collecting logs may collect PII and other personal data about employees, but only for the purpose of providing the service.

CONTROL 09

Email and Web Browser Protections

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.

Privacy Applicability

Email is the most common method of business communication, and email servers store all emails sent by users from their work accounts. Browsers are also key business applications and are required for everyday workplace activities. Most of the Safeguards within this Control can help protect an enterprise's personal data, but browser extensions and DNS filtering have an outsized privacy impact and should be carefully considered.

Privacy Implications

- Browser extensions are privileged apps running within a browser. They can granularly track users, view previous browser history, read cookies, and inject content into webpages.
- Tracking cookies and other elements as well as fingerprinting can be used by sites to "follow and record" all the sites visited by a user.
- URL filters help prevent an enterprise asset from accessing network resources that the enterprise deems unfit for the enterprise. URL filtering will also allow the filter to track the resources accessed or attempted to be accessed by users on the network.
- Email servers store extremely sensitive information about employees, customers, and others. Also, email accounts are often used to support password reset or two-factor authentication for other accounts. Retaining too much information on these servers for too long may make a breach worse.
- DNS servers can granularly track a user's network activity. Most large enterprises have gateways for protection and monitoring of email and web traffic, which store activity about web searches, and may be another repository of emails. DNS filtering offers benefits, but who is doing the filtering and how they are doing it can have privacy implications. They can stop others from tracking you, but also allow the enterprise owning the DNS server to exclusively track users. It is worth understanding who that organization is, what their privacy policy is, and what their reputation is in the community. Also, given the sensitive nature of data handled by DNS servers, their data in transit and stored needs to be appropriately secured.

Data Collection

Web browsers can store local histories of all sites visited by the user. Some browser extensions are known to collect data from users without their knowledge. Websites may also track users with cookies, other tracking elements, and/or by fingerprinting. Systems performing URL filtering and DNS functions will know the websites that specific users and clients visit on the network. It would be trivial for these systems to collect and store user data.

Data Storage

By default, browser history will be stored on a user's computer. This information may also be federated across all systems logged into the browser with that username and password via modern history and bookmark synching. Some browsers offer profiles, containers, and other portioning features to help a user keep their browsing activity safe. DNS and URL filtering data should be considered sensitive and appropriately secured in a manner similar to other sensitive data the enterprise holds. Such data should only be collected if necessary.

Additional Discussion

Most of the Safeguards within this Control do not have direct privacy implications. With that said, refraining from implementing many of the Safeguards within this Control may lead to a successful attack on an enterprise. This includes defenses such as regularly updating browsers and email clients (Safeguard 9.1), implementing Domain-based Message Authentication, Reporting & Conformance (DMARC) (Safeguard 9.5), and blocking specific file types (Safeguard 9.6).

Browser extensions can have both privacy benefits and drawbacks. Since browser extensions are essentially software, with elevated privileges, running within a browser, they are able to access more information about a browser session and the user than is typical. Browser extensions can mask certain activities to actually enable privacy such as HTTPS Everywhere and Privacy Badger. Enterprises are encouraged to have an Allowlist of approved security and privacy-based browser extensions to aid their employees. These extensions should be vetted by IT, cybersecurity, and privacy business units within an enterprise.

Yet, browser extensions can also granularly track users, view previous browser history, read cookies, and inject content into webpages. For instance, one academic study from 2018 states that of the "...178,893 extensions crawled from the Chrome Web Store between September 2016 and March 2018..." the "...top 10 most popular Chrome extensions that we confirmed to be leaking private/sensitive information have [sic] more than 60 million users combined." [5] Further, some browser extensions could contain malware. It is generally best to assume that a browser is accessing data the user is not intending and refrain from using untrusted browser extensions to the degree practical as mentioned in Safeguard 9.4.

Fair Information Practice Principles

- **The Collection Limitation Principle.** Browsers and email systems should be configured to collect as little PII and personal data from employees as possible. Local regulations may require certain data to be recorded for specific purposes.
- **The Data Quality Principle.** Data from browsers and email systems should only be used for legitimate security purposes. For example, serving ads to users based on text within an email or their browsing could violate this principle.
- **The Purpose Specification Principle.** Employees should be informed what information may be stored by browsers and email, and how the information will be used.
- **The Use Limitation Principle.** Employees should be informed if browser and email data will be transferred to other systems owned by third-party service providers, such as a marketing company, or otherwise used by third-parties and why.
- **The Security Safeguards Principle.** Care should be taken to secure any browser and email data both when stored and in transit, which likely includes PII and other personal data.
- **The Openness Principle.** Employees with PII and other personal data collected by enterprise systems should understand what external systems may contain their personal data and why.

5 CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, October 2018 Pages 1687–1700 https://doi.org/10.1145/3243734.3243823

- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be collected from browsers and email clients by an enterprise. A lawful basis is needed for collecting personal data.
- **Purpose limitation.** Users should be informed in writing about the purpose of collecting personal data from browsers and email from the outset of collecting it. Personal data obtained through the application of this Control should only be used for this system and employees should be informed if their information will be transferred to other systems owned or used by third-party service providers. This includes network visibility and security tools. Serving ads to users based on their web history or text within an email could violate this principle.
- **Data minimization.** Browsers and email systems must be configured to collect as little PII and personal data from employees as possible. In addition to GDPR requirements, other local regulations may require certain data to be recorded.
- **Accuracy of data.** User data collected from browsers and email clients should be regularly checked for accuracy. Written processes should be documented for how to maintain this data and how incorrect data can be corrected.
- **Storage limitation.** User data from browsers and email clients should only be stored for as long as needed. Browser and email data may be quite useful in incident response scenarios, and therefore kept for a significant amount of time. Obsolete data should be deleted without delay.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Control 3. A user's browser and email data should be protected from unauthorized access, modification, and disclosure and can be leveraged by an attacker to obtain unauthorized access to an enterprise's systems. This is especially true for email, as records of authentication systems may be included there.

Control 9 Privacy Applicability Table

CIS Control 09: Email and Web Browser Protections				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
9.1	Applications	Protect	**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.	**No** Browsers and email clients that are unsupported should not be used. This is not included because this enhances security with no specific privacy impact. Users should be offered the ability to offer privacy preserving browsers.
9.2	Network	Protect	**Use DNS Filtering Services** Use DNS filtering services on all enterprise assets to block access to known malicious domains.	**Yes** DNS filtering can help prevent tracking by known malicious domains, but also gives the filter complete knowledge of the sites a user visits. Turning off DNS logging would be a more privacy preserving action, but may conflict with other IT needs.

CIS Control 09: Email and Web Browser Protections				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
9.3	Network	Protect	**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.	**Yes** This practice can help prevent an enterprise asset from downloading malware that may result in a privacy exposure. Yet, this network filter will have deep knowledge on how users are accessing the enterprise network. Turning off logging would be a more privacy preserving action but may conflict with other IT needs.
9.4	Applications	Protect	**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.	**Yes** Browser extensions are well known for accessing and sharing information that users did not intend. Some browser extensions offer privacy preserving features.
9.5	Network	Protect	**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.	**No** DMARC can prevent phishing emails and other malicious emails from reaching users, but there is no specific privacy impact.
9.6	Network	Protect	**Block Unnecessary File Types** Block unnecessary file types attempting to enter the enterprise's email gateway.	**No** Blocking the transfer of file types is important, but there is no specific privacy impact.
9.7	Network	Protect	**Deploy and Maintain Email Server Anti-Malware Protections** Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.	**Yes** Scanning emails can prevent phishing emails and other malicious attachments from reaching users, but this system will also be able to access personal data about a user and other individuals.

CONTROL 10

Malware Defenses

OVERVIEW

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

Privacy Applicability

This Control is specific to technologies and processes to prevent a successful attack from malware. There are few direct privacy impacts of implementing the malware protection Safeguards contained within this Control. When malware is installed on a system, it may collect PII and other personal data (e.g., contacts, browser history).

Privacy Implications

- Spyware and adware may track what a user is doing on an infected computer. Other types of malware may also perform this function while performing more malicious activities on a system.
- Anti-malware software often requires elevated privileges on a system. This software could be abused by both the developer of the anti-malware software, and also by whoever administers the software. That administrator is also likely to have other types of privileged access over the system.
- If host and perimeter malware tools record sensitive data, any alerts and logs generated by these systems could contain that private information.

Data Collection

Malware infecting a system might collect and send private or personal data to the malware developer. This information may also be sent outside of the network. Defensive malware tools may also collect private information. Administrators should work with corporate Privacy Officers or the applicable business unit to understand what potential data is stored in logs and alerts.

Data Storage

Malware may be used to steal personal information and hold it elsewhere outside of the network. The logs and alerts from defensive anti-malware software should be stored in a secure location and access should be restricted.

Additional Discussion

Malware protections can ultimately help enable privacy. Without some sort of malware defense, and the regular updates to keep these defenses effective, the system is much more vulnerable to attack. Once infected, all local and network activity may be tracked and potentially exfiltrated elsewhere.

It is common for employees, including IT staff, to download software outside of the explicit approval of IT policy. Depending on the site hosting the software download, downloading the correct software can be intentionally confusing, and users may accidentally download spyware/malware in lieu of anti-malware software.

Fair Information Practice Principles

- **The Collection Limitation Principle.** Anti-malware and perimeter defense systems should be configured to collect as little PII and personal data from employees as possible.
- **The Data Quality Principle.** Data from anti-malware and perimeter defense systems should only be used in security processes for defending against malware.
- **The Purpose Specification Principle.** Employees should be informed about the information that may be stored by anti-malware and perimeter defense systems, as well as how the information will be used.
- **The Use Limitation Principle.** Employees should be informed if anti-malware and perimeter defense data will be transferred to other systems owned or used by third-party service providers, such as a marketing company.
- **The Security Safeguards Principle.** Care should be taken to secure any anti-malware and perimeter defense data, which likely includes PII and other personal data.
- **The Openness Principle.** Employees with PII and other personal data collected by enterprise systems should understand what external systems may contain their personal data and why.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be collected by an antivirus system. A lawful basis is needed for collecting personal data.
- **Purpose limitation.** Users should be informed in writing about your purpose for collecting personal data in the anti-malware platform from the outset of collecting it. Personal data collected through the anti-malware platform should only be used for this system and employees should be informed if their information will be transferred to other systems owned by third-party service providers.
- **Data minimization.** User data collected via an anti-malware platform is likely incidental, or a personal file may have been infected or was an infection vector. There will likely be significant overlap with the information collected for the enterprise asset and software inventories.
- **Accuracy of data.** User data collected via this Control should be regularly checked for accuracy.
- **Storage limitation.** User data, such as PII, should only be stored for as long as needed in an anti-malware system. Obsolete data should be deleted without delay.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Controls 3, 4, and 5. User data collected should be protected from unauthorized access, modification, and disclosure and can be leveraged by an attacker to obtain unauthorized access to an enterprise's systems.

Control 10 Privacy Applicability Table

CIS Control 10: Malware Defenses				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
10.1	Devices	Protect	**Deploy and Maintain Anti-Malware Software** Deploy and maintain anti-malware software on all enterprise assets.	**Yes** Research should be done to understand the information anti-malware software can access on a system and take privacy into account in its implementation.
10.2	Devices	Protect	**Configure Automatic Anti-Malware Signature Updates** Configure automatic updates for anti-malware signature files on all enterprise assets.	**Yes** Administrators for this software may have access to sensitive information.
10.3	Devices	Protect	**Disable Autorun and Autoplay for Removable Media** Disable autorun and autoplay auto-execute functionality for removable media.	**No** There are no direct privacy impacts with disabling autorun.
10.4	Devices	Detect	**Configure Automatic Anti-Malware Scanning of Removable Media** Configure anti-malware software to automatically scan removable media.	**Yes** The anti-malware software may scan personal files and collect information from these files. This personal data may subsequently be provided to an administrator for review.
10.5	Devices	Protect	**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™.	**No** Although these features may prevent a user from installing their own operating system on the hardware, there are no direct privacy impacts.
10.6	Devices	Protect	**Centrally Manage Anti-Malware Software** Centrally manage anti-malware software.	**Yes** Administrators for this software will likely have access to PII and personal data.
10.7	Devices	Detect	**Use Behavior-Based Anti-Malware Software** Use behavior-based anti-malware software.	**No** Certain benign user behaviors may trigger an administrator to personally review logs.

CONTROL 11

Data Recovery

OVERVIEW

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

Privacy Applicability

This Control is meant to assist enterprises in preparing to recover from a cyber incident. Privacy concerns exist with many of the Safeguards within this Control. Principally, the Safeguards associated with providing information to third-parties are most applicable.

Privacy Implications

- IT staff will need to create backups of enterprise information as part of this Control. PII contained within human resource (HR) and other records will need to be backed up, yet PII and other personal data may incidentally also be collected as part of this process. This is likely unavoidable unless both IT staff and employees are diligent about not storing non-work-related information on company systems. But, even work-related information in backups are likely to contain personal data. It's common for these backups to then be stored with companies specializing in disaster recovery.
- Depending on the security measures taken by internal IT staff, third-party organizations involved in disaster recovery scenarios may have access to data stored in backups.
- Testing if backups can actually be restored is an important part of a data recovery process. Restoring backups during testing should be done carefully. If sensitive data is restored, that system should be properly protected and securely deleted after the exercise is complete.

Data Collection

PII and other personal data may be collected by IT when performing backups, and transferring backups offsite, or to a third-party organization for safekeeping and ransomware protection. Specific security protections for PII and other personal data need to be stipulated in the service level agreement (SLA).

Data Storage

IT may store backups offsite at an enterprise-owned location, such as another office building that is geographically separated from the primary office. Third-party organizations providing storage for company backups may store the information in a cloud platform or at a physical hot site or cold site. Personal data at both locations needs to be protected.

Additional Discussion

When performing backups, the ultimate storage location can make a difference. For instance, if backups are stored in the European Union, specific requirements related to protection of PII and other personal data will be required per General Data Protection Regulation (GDPR). Once a backup is taken, it's best practice to ensure that the intended data is being saved and that it can actually be used to recover from a data loss. The testing and restoration of backups should be done in an organized and careful manner, as IT has access to PII and other personal data. If sensitive data is restored, the system should be properly protected until it is securely deleted.

Fair Information Practice Principles

- **The Collection Limitation Principle.** All information on a system should not be backed up unless there is a strict delineation of enterprise and user data.
- **The Data Quality Principle.** Data from backups should only be used during data recovery or testing.
- **The Purpose Specification Principle.** Employees should be informed what information may be backed up and how the information will be used.
- **The Use Limitation Principle.** Employees should be informed if backups will be transferred to other systems owned or used by third-party service providers, such as a company focusing on data recovery.
- **The Security Safeguards Principle.** Care should be taken to secure any backups that likely include PII and other personal data. This includes encrypting the backups and ensuring adequate access control mechanisms are in place.
- **The Openness Principle.** Employees with PII and other personal data collected by enterprise systems should understand what external systems may contain their personal data.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be collected during a backup or backup testing process. A lawful basis is needed for collecting personal data.
- **Purpose limitation.** Users should be informed in writing about your purpose for collecting personal data during a backup. Personal data collected during this process may be transferred to other vendors to assist in disaster recovery or long-term data storage. Employees should be made aware of this.
- **Data minimization.** Nothing more than is necessary for restoration of enterprise services should be collected, but there may be incidental collection of personal data. This should be avoided and written processes should be in place to avoid personal data collection.
- **Accuracy of data.** Backup data should regularly be verified for integrity in utility. Written processes should be documented for how user data in backups is maintained and how incorrect data can be corrected or, more likely, removed.
- **Storage limitation.** User data should only be stored for as long as needed, if it is needed at all. Obsolete data should be deleted without delay.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Controls 3, 4, and 5. Personal data should be protected from unauthorized access, modification, and disclosure and can be leveraged by an attacker to obtain unauthorized access to an enterprise's systems.

Control 11 Privacy Applicability Table

CIS Control 11: Data Recovery				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
11.1	Data	Recover	**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.	**Yes** This process should take privacy into account and ensure that to the extent possible, PII and other personal data are not backed up, or at least not provided to third-parties in an insecure form.
11.2	Data	Recover	**Perform Automated Backups** Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	**Yes** Automated backups should not store PII and other personal data in a form that third parties can access without the consent of the data owner.
11.3	Data	Protect	**Protect Recovery Data** Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	**Yes** Any PII and other personal data that is backed up should be protected at least as well as enterprise data. In some cases, it may require higher data security.
11.4	Data	Recover	**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.	**Yes** There are no privacy implications of having an offsite backup of enterprise data if it is secure and access is restricted.
11.5	Data	Recover	**Test Data Recovery** Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.	**Yes** Restoring backups should be done carefully. If sensitive data is restored as part of the testing process, that system should be properly protected and securely deleted.

CONTROL 12

Network Infrastructure

OVERVIEW

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

Privacy Applicability

The Safeguards within this Control pertain to ensuring network infrastructure (e.g., firewalls, routers, switches) is appropriately set up, maintained, and configured throughout their lifecycle. Multiple Safeguards focus on using up-to-date software on network appliances and modern, secure administration protocols. As such, many of the Safeguards within this Control do not have a direct privacy impact.

Privacy Implications

- Network infrastructure will likely be able to granularly track user activity throughout the network.
- Improper network design and segmentation could lead to lesser degrees of privacy for enterprise network users. Failure to document decisions that are meant to enhance privacy could hamper future developments in a burgeoning privacy program.
- Logs relating to authentication and authorization systems in general may record private action. For instance, some centralized authentication systems log the geolocation of users when they connect. Other authentication events will trigger log entries, such as time of access, time of authentication attempt, and what resources were accessed. Collecting these log entries can be beneficial to investigative efforts during incident response; however, they can also be used to thwart privacy. Due to this and other factors, it's best practice to regularly audit and verify who has access to personal data.

Data Collection

No PII or personal data should be intentionally collected within this Safeguard by network infrastructure. This includes decrypting employee traffic, which was specifically removed from the CIS Controls as a privacy protecting measure. Yet, many systems will collect data that could be used for tracking while performing their security or privacy function.

Data Storage

In general, network infrastructure should not store PII and personal data. With that said, some network systems will observe what sites and resources users are accessing both internally and externally on the internet. These network appliances include DNS, intrusion detection system (IDS), and firewalls. Since web history can be considered privacy-relevant data, if such information is necessary for securing network infrastructure, this information should be stored in a secure fashion and only for as long as is needed.

Additional Discussion

Planning and implementing a secure architecture (Safeguard 12.2 – Establish and Maintain a Secure Network Architecture) can help to enable privacy across an enterprise. This ensures there are architectural elements in the network that prevent access to employee systems and information (to include mobile devices). Many layers of physical and logical defenses need to be put into place for this to function appropriately. This includes the centralization of authentication systems, privilege management, remote network access, and preventing systems on one portion of the network from accessing another unrelated network segment. Privacy decisions and other considerations designed into the network should be explicitly documented to ensure that other IT staff understand these decisions and can follow them going forward. This documentation can also be useful for the legal team if a breach occurs in the future.

There are often regulatory requirements, or third-party agreements for security controls on devices that route personal data within or between networks. Regular auditing of regulatory and third-party agreement requirements can help verify the location and appropriate protection of all PII and other personal data. In a similar manner, as part of personal plan and data governance, ensure that all PII or other privacy data is identified, and the appropriate data flows are known. That way, appropriate protection can be applied to all systems in the data flow chain.

Fair Information Practice Principles

- **The Collection Limitation Principle.** Network infrastructure should not be intentionally configured to collect PII and other personal data.
- **The Data Quality Principle.** PII and other personal data collected from network devices should only be used for making security decisions for network access and information filtering.
- **The Purpose Specification Principle.** Employees should be informed what information will be collected by network devices and how the information will be used.
- **The Use Limitation Principle.** Employees should be informed if data collected by network devices will be transferred to other systems owned or used by third-party service providers, such as a company focusing on network forensics or incident response.
- **The Security Safeguards Principle.** Care should be taken to secure any network data that likely includes PII and other personal data.
- **The Openness Principle.** Employees with PII and other personal data collected by enterprise systems should understand what external systems may contain their personal data.
- **The Individual Participation Principle.** This is unlikely to be implemented without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be collected by network infrastructure. A lawful basis is needed for collecting personal data.
- **Purpose limitation.** Network infrastructure should not be intentionally configured to collect PII and other personal data. Users should be informed in writing about any network infrastructure collecting personal data.

- **Data minimization.** Personal data should not be collected by network infrastructure unless it is necessary. Written processes should be in place to avoid undesirable personal data collection.
- **Accuracy of data.** Any personal data should be maintained with written processes documented for how user data is maintained and how incorrect data can be corrected or, more likely, removed.
- **Storage limitation.** User data should only be stored for as long as needed, if it is needed at all. Obsolete or unnecessary user data should be deleted without delay.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Control 3 – Data Protection for protecting backups. Personal data should be protected from unauthorized access, modification, and disclosure and can be leveraged by an attacker to obtain unauthorized access to an enterprise's systems.

Control 12 Privacy Applicability Table

CIS Control 12: Network Infrastructure

Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
12.1	Network	Protect	**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.	**No** Network infrastructure should be kept up-to-date, but there is no specific privacy impact with the implementation of this Safeguard.
12.2	Network	Protect	**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.	**Yes** A secure architecture can help to enable privacy by preventing access to employee systems and information. This can be via privilege management or preventing systems on one portion of the network from accessing another network segment.
12.3	Network	Protect	**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.	**No** Systems containing personal data will need routine maintenance and administration. These systems should only be accessed via secure protocols. No specific privacy impact for this Safeguard.
12.4	Network	Identify	**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.	**Yes** Privacy protections and considerations designed into the network should be explicitly documented.
12.5	Network	Protect	**Centralize Network Authentication, Authorization, and Auditing (AAA)** Centralize network AAA.	**Yes** Centralized AAA will likely record and log information about a user's current location.
12.6	Network	Protect	**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).	**No** This Safeguard should be applied to protect all information throughout a network, but there is no specific privacy impact.

CIS Control 12: Network Infrastructure

Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
12.7	Devices	Protect	**Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure** Require users to authenticate using MFA to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.	**Yes** Information systems associated with remote login or VPN capabilities will likely learn information about a user's current location. VPNs may track a user's geographical location.
12.8	Devices	Protect	**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.	**Yes** Administrators are encouraged to use separate devices for administrative tasks and day-to-day work-related tasks. Devices and applications that don't require internet access should either be air-gapped or placed into a private network that doesn't allow them access to external networks.

CONTROL 13

Network Monitoring and Defense

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.

Privacy Applicability

Ensuring visibility into a network is essential in understanding the types and frequency of attacks facing an enterprise. Network visibility, and acting on this information, is ultimately the goal of this Control. To accomplish this, the Network Monitoring and Defense Safeguards focus on installing, configuring, and monitoring software products that sit on the network and on the host. These products will have privileged access to information on the network and host, and what information they access, store, and use can have privacy implications. Many of these Safeguards have privacy impacts.

Privacy Implications

- Enterprises should ensure that SIEMs are not regularly alerting on information that contains personal data and is thus being pushed up to security analysts for manual review. That is distinct from SIEMs alerting IT on the existence of personal information and cleartext passwords.
- Network infrastructure will likely be able to granularly track user activity throughout the network.
- Perimeter defense and other network architecture systems may collect information about their customers.

Data Collection

Network traffic information collected by IDS, intrusion prevention system (IPS), and application filtering software, alongside alerts generated from a variety of sources, may be collected.

Data Storage

Network traffic information collected by IDS, IPS, and application filtering software, alongside alerts generated from a variety of sources, must all be stored. The owners of the software for all of these systems likely have access to all of this information and may store this information within their own private network. The enterprise using these systems will also store this information, and it should be appropriately protected.

Additional Discussion

Best practice implementation of centralizing logs and alerts requires the usage of a SIEM tool (Safeguard 13.1 – Centralize Security Event Alerting). Many of the other Safeguards within this Control focus around implementing products that ultimately produce logs and alerts that can be ingested into a SIEM. It is quite possible that there would be privacy issues with the type of data collected by these perimeter defense systems, especially user activity, email logs, and personal information that can be logged when a user visits a website. Because of this, it is best to ensure that there is a data governance process that identifies and protects all PII or personal data and where that data flows in and out of the network.

Mobile devices should also be part of this process, and some of the perimeter defense tools do have mobile subcomponents or entirely separate product categories that could be applicable, such as mobile threat defense. Finally, remember that insufficient perimeter defense controls could prove lack of sufficient defenses to protect personal data, as required by some regulatory frameworks.

Fair Information Practice Principles

- **The Collection Limitation Principle.** Network infrastructure should not be intentionally configured to collect PII and other personal data.
- **The Data Quality Principle.** PII and other personal data collected from network devices should only be used for making security decisions for network access and information filtering.
- **The Purpose Specification Principle.** Employees should be informed what information will be collected by network devices and how the information will be used.
- **The Use Limitation Principle.** Employees should be informed if data collected by network devices will be transferred to other systems owned or used by third-party service providers, such as a company focusing on forensics or incident response.
- **The Security Safeguards Principle.** Care should be taken to secure any network data that likely includes PII and other personal data.
- **The Openness Principle.** Employees with PII and other personal data collected by enterprise systems should understand what external systems may contain their personal data.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be collected by network infrastructure. A lawful basis is needed for collecting personal data.
- **Purpose limitation.** Network infrastructure should not be intentionally configured to collect PII and other personal data. Users should be informed in writing about any network infrastructure collecting personal data. Sharing data with third-parties should be avoided if possible, and users should understand what is being shared with whom.
- **Data minimization.** Personal data should not be collected by network infrastructure unless it is necessary. Written processes should be in place to avoid undesirable personal data collection.
- **Accuracy of data.** Any personal data should be maintained with written processes documented for how user data in backups is maintained and how incorrect data can be corrected or, more likely, removed.
- **Storage limitation.** User data should only be stored for as long as needed, if it is needed at all. Obsolete or unnecessary user data should be deleted without delay.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Control 3: Data Protection for protecting backups. Personal data should be protected from unauthorized access, modification, and disclosure and can be leveraged by an attacker to obtain unauthorized access to an enterprise's systems.

Control 13 Privacy Applicability Table

CIS Control 13: Network Monitoring and Defense				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
13.1	Network	Detect	**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.	**Yes** Administrators should work with the enterprise privacy officer, or legal department, to understand what potential PII is stored in logs and alerts and how it should be protected.
13.2	Devices	Detect	**Deploy a Host-Based Intrusion Detection Solution** Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.	**Yes** Research should be done to understand the information host-based IDS can access on a system and specifically whether it can access any personal data.
13.3	Network	Detect	**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.	**Yes** Research should be performed to understand how the IDS solution stores and collects information about individual users.
13.4	Network	Protect	**Perform Traffic Filtering Between Network Segments** Perform traffic filtering between network segments, where appropriate.	**Yes** Traffic filtering should in theory increase privacy for individual users and systems.
13.5	Devices	Protect	**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.	**No** Although this Safeguard can help prevent a breach, there are no direct privacy impacts. If there is a remote agent stored on the user's asset, then that agent may be able to access user data and this Safeguard would apply.
13.6	Network	Detect	**Collect Network Traffic Flow Logs** Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.	**Yes** Flow logs will contain detailed information about resources accessed by specific IP addresses, some of which may be statically assigned, alongside protocols used to access those resources.
13.7	Devices	Protect	**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.	**Yes** Research should be done to understand the information host-based IPS can access on a system and whether there are any privacy implications associated with the deployment.
13.8	Network	Protect	**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.	**Yes** Research should be done to understand the information host-based IPS can access on a system and whether there are any privacy implications associated with the deployment.

CIS Control 13: Network Monitoring and Defense				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
13.9	Devices	Protect	**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.	**No** There are no privacy impacts of using port-level access control for network access.
13.10	Network	Protect	**Perform Application Layer Filtering** Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.	**Yes** While these tools can help enable privacy by preventing a breach, they may learn and store detailed information about individual users. Where that data is stored and how it is treated is also a concern.
13.11	Network	Detect	**Tune Security Event Alerting Thresholds** Tune security event alerting thresholds monthly, or more frequently.	**Yes** If alerts are exposing or storing sensitive information, the thresholds should be appropriately tuned. Ensure alerts are communicated in a secure manner.

CONTROL 14

Security Awareness and Skills Training

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.

Privacy Applicability

This Control is intended to ensure that employees and contractors receive security training targeted toward their particular role and responsibilities. Security awareness training often includes privacy as a component of the overall curriculum, but due to the scope of this *Privacy Guide,* this Control will be viewed through the lens of performing privacy awareness training. As such, many of the Controls are directly applicable.

Privacy Implications

- IT administrators with enhanced privileges and access may make poor privacy decisions if they are not trained on appropriate use of their access and consequences of privacy breaches or violations. IT staff appropriately configuring systems across the enterprise to refrain from collecting certain types of PII and other personal data is an opportunity to make a large, positive privacy impact.
- Failure to provide privacy awareness training may conflict with existing regulation and other compliance requirements.
- Users should understand the privacy policies of the enterprise and how to appropriately protect their own information.
- Contractors and third-party service providers should understand the privacy requirements mandated by the organization. Ultimately, this is up to the primary enterprise to communicate privacy requirements and ensure they are met.

Data Collection

PII and other personal data may not be specifically collected for this Control, with the exception of which individuals successfully completed privacy training.

Data Storage

The list of which employees completed privacy training is likely not the highest priority for securing. Yet, this information could still be valuable to an attacker (e.g., for phishing) and should be appropriately protected.

Additional Discussion

Note that security awareness training on its own is not necessarily a substitute for privacy awareness training, although security awareness training seminars are a great time to also provide privacy training. All employees should be specifically trained for privacy impacts to employees and contractors in the workplace. Different roles will require specific types of training, as certain roles will have access to PII, whereas other roles will have access to other types of sensitive information. Developers, system engineers, and software architects may need dedicated training in privacy engineering.

How that data is used, and protected, could be unique as there may be specific regulatory compliance policies that need to be followed. This is especially true for those job functions that regularly work with PII and other sensitive information. Training should occur at all levels of technical staff on privacy, socializing privacy policies to users, and promoting good behavior in protecting privacy information.

Privacy training should encompass multiple topics. One of the most important topics is providing an understanding of how to identify personal data or data that could be considered personal data, especially if combined with other data. The following are also relevant topics that can be included:

- Understanding what data may be labeled sensitive under any applicable regulatory frameworks and compliance requirements
- Addressing personal data on mobile devices, including BYOD
- How to prevent, report, and mitigate a breach of personal data
- Precautions for handling different types of personal data
- The risks of de-identified data being re-identified
- How to use de-identified aggregate data rather individual data to achieve the same purpose
- The enterprise's current policies surrounding the protection of private information

This privacy awareness training should receive regular updates, and employees should retake the training at regular intervals. The enterprise should track attendance and completion of training.

The Department of Homeland Security provides a resource for privacy training. These include major federal statutes, guidelines, and policies related to privacy in the United States. Additionally, ideas are provided for promoting privacy awareness, and measuring success for training activities. The US Nuclear Regulatory Commission's (NRC) privacy training can be a useful example for enterprises beginning to perform privacy training, as can the State of California Department of Aging.

Fair Information Practice Principles

- **The Collection Limitation Principle.** N/A
- **The Data Quality Principle.** N/A
- **The Purpose Specification Principle.** N/A
- **The Use Limitation Principle.** N/A
- **The Security Safeguards Principle.** N/A
- **The Openness Principle.** N/A
- **The Individual Participation Principle.** N/A
- **The Accountability Principle.** N/A

General Data Protection Regulation Principles

The GDPR principles don't specifically apply to cybersecurity training and awareness, but employees should be made aware of any responsibilities they have under GDPR. This may be specific to certain employees working on products used by EU citizens.

- **Lawfulness, fairness, and transparency.** N/A
- **Purpose limitation.** N/A
- **Data minimization.** N/A
- **Accuracy of data.** N/A
- **Storage limitation.** N/A
- **Integrity and confidentiality.** N/A

Control 14 Privacy Applicability Table

CIS Control 14: Security Awareness and Skills Training

Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
14.1		Protect	**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.	**Yes** Establishing and maintaining a privacy training program is a critical part of an enterprise protecting PII and other sensitive information.
14.2		Protect	**Train Workforce Members to Recognize Social Engineering Attacks** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.	**Yes** Employees should understand when someone is attempting to obtain PII and other personal data from individuals or the enterprise.
14.3		Protect	**Train Workforce Members on Authentication Best Practices** Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	**Yes** Certain methods of authentication are more privacy preserving than others.
14.4		Protect	**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.	**Yes** Employees with responsibilities pertaining to PII and other personal data should receive specific training for how to handle this data. The enterprise can also choose to train the workforce on privacy tools and practices, such as using privacy features of browsers, camera covers, and more.
14.5		Protect	**Train Workforce Members on Causes of Unintentional Data Exposure** Train workforce members to be aware of causes for unintentional data exposure. Example topics include misdelivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.	**Yes** Employees with responsibilities pertaining to PII and other personal data should receive specific training for how to recognize unintentional data exposure.

CIS Control 14: Security Awareness and Skills Training				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
14.6		Protect	**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.	**Yes** Employees need to receive specific training about recognizing security and privacy incidents related to PII.
14.7		Protect	**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.	**No** Although an important security control, there is no specific action to take here for private information.
14.8		Protect	**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.	**Yes** Employees should understand the dangers of sending personal data without the appropriate security controls protecting that data and know how to avoid making that mistake.
14.9		Protect	**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.	**Yes** Employees with responsibilities pertaining to PII and other personal data should receive specific training for how to handle their personal data.

CONTROL 15

Service Provider Management

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.

Privacy Applicability

It is quite common for an enterprise to leverage cloud service providers (CSPs) for email or storage. This Control covers actions that should be taken to ensure that third-party service providers are properly securing their customer's data, and their own systems. The recommended measures for this Control include understanding what service providers are in use, what types of data they store, and monitoring their performance. All of these activities are applicable to privacy, as it is common for third-party service providers to store and process PII and other personal data, such as is the case with HR information. Each Safeguard within this Control can be successfully applied to privacy. When possible, consider choosing providers that have privacy certifications or some other independent auditing of their own privacy practices.

Privacy Implications

- Service providers may utilize, sell, or share PII and other personal data obtained via their customers.
- Personal data could be provided directly as part of a business function or created via the use of a product or service such as the case for firewalls or other network appliances. In both cases, the owner of the personal data has a responsibility to keep this information from being disclosed. Examples of sensitive information that may be handled by third-party organizations include:
    - HR records and other PII
    - Log files for workstations, servers, and network appliances
    - DNS records
    - URL filtering data
    - Hardware, software, data, and other types of inventories

Data Collection

What data can be collected by a service provider is an extremely important question to settle before a service is used. Data that the service provider is able to collect should be clearly stated in service-level agreements (SLAs). Specific types of data should be discussed, as should be whether the service provider can use your data within their products or sell the data to other organizations.

Data Storage

Security controls relating to the security of PII and other personal data should be explicitly written and agreed upon before usage.

Additional Discussion

Third-party service providers are breached from time to time, and their customers' data may be included in this breach. It is important to keep a handle on the data collection and security controls that service providers have in place. Informing them of privacy expectations at the outset of any discussions about business partnerships may be worthwhile, as they may be unable to comply with certain privacy regulations. The geographic location that a service provider operates out of likely dictates the privacy rules they must adhere to. It may be wise to choose a service provider from a jurisdiction without privacy or data protection laws unless they can demonstrate that they adhere to high data protection standards through external certification or other trusted mechanism.

Fair Information Practice Principles

- **The Collection Limitation Principle.** Service providers should not collect PII and other personal data, unless required.
- **The Data Quality Principle.** PII and other personal data collected by service providers or shared by the enterprise with service providers (as needed) should only be used while providing the product or service they were contracted for.
- **The Purpose Specification Principle.** Employees should be informed what information will be collected by service providers and how the information will be used.
- **The Use Limitation Principle.** Employees should be informed if data collected by service providers will be transferred to other systems owned by third-party service providers.
- **The Security Safeguards Principle.** Care should be taken to secure any shared data.
- **The Openness Principle.** Employees with PII and other personal data collected by enterprise systems should understand what external systems may contain their personal data.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be shared to a third-party service provider. A lawful basis is needed for collecting personal data, and this service provider may need to comply with GDPR regulations if they are acting on your behalf and processing data from specific individuals.
- **Purpose limitation.** Employees should be informed what information will be collected by service providers and how the information will be used. Third-party service providers should not have the ability to access more information than they require.
- **Data minimization.** Third-party service providers should not have the ability to access more information than they require. Written processes and contracts should be in place to avoid undesirable personal data collection by service providers.
- **Accuracy of data.** Any personal data shared with service providers should be maintained with written processes documented for how user data in backups is maintained and how incorrect data can be corrected or, more likely, removed. Service providers must implement these same procedures.
- **Storage limitation.** User data should only be stored for as long as needed, if it is needed at all. Obsolete or unnecessary user data should be deleted without delay.

- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Control 3 and Control 15. Specifically, obtaining evidence that any service provider is leveraging a security framework is necessary.

Control 15 Privacy Applicability Table

CIS Control 15: Service Provider Management				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
15.1		Identify	**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.	**Yes** An inventory of which service providers store what types of PII and personal data should be developed and maintained.
15.2		Identify	**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.	**Yes** Privacy expectations should be built into this service provider management policy.
15.3		Identify	**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.	**Yes** Providers can be classified based on access to PII, personal data, and any regulations that would be applicable specifically due to personal data.
15.4		Protect	**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; and must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.	**Yes** For this Safeguard, it is recommended that privacy requirements also be included within service provider contracts.
15.5		Identify	**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 Organizational Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaire, or other appropriately rigorous process. Reassess service providers annually, at a minimum, or with new and renewed contracts.	**Yes** Enterprises should assess their service providers and their defensive mitigations used to protect PII and other personal data.

CIS Control 15: Service Provider Management				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
15.6	Data	Detect	**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.	**Yes** Periodic assessment of service provider storage, collection, and handling of PII and other personal data should be performed.
15.7	Data	Protect	**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.	**Yes** Once a service provider is no longer being actively used, PII and other personal data should be securely deleted from their systems.

CONTROL 16

Application Software Security

OVERVIEW

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

Privacy Applicability

This Control principally focuses on efforts that software architects and developers can take to prevent exploitable vulnerabilities in their code. These exploitable vulnerabilities could potentially lead to unauthorized exposure of PII and other personal data. With that said, most of the Safeguards contained within this Control are not directly related to protecting PII. Therefore, they will be listed as not applicable.

Privacy Implications

- All developers should be trained on privacy requirements pertaining to software handling PII and other personal data and how to include privacy in the design of software.
- Third-party software libraries, components, and application programming interfaces (APIs) may collect information that they process. They may also fingerprint users, which could be used for tracking.
- Applications might have logging or error messages that write data to help identify and troubleshoot problems. There is a chance that some of this data might have privacy requirements; it is important to evaluate all logs, backups, and cache stores where privacy data might be permanently or temporarily stored.
- Failure to provide or require appropriate security controls to third-party software developers with access to PII and other personal data.

Data Collection

Third-party software libraries and application programming interfaces (APIs) may collect information through their usage, such as is the case with log data. Data that these third-party components can collect should be clearly stated in SLAs. Implement regular auditing of regulatory and third-party agreement requirements to verify who has access to privacy data.

Data Storage

Security controls relating to the security of your data should be explicitly written down and agreed upon with third-party component providers before usage. Ensure there are data governance processes that identify all PII or privacy related data, where it is stored, and who should have access. Apply controls and monitoring to these accounts.

Additional Discussion

The software development processes used by the company should identify any additional tasks that need to be accomplished when writing software handling PII, and software engineers should be trained on handling PII and other personal data. When designing software, additional scrutiny should be provided to applications, modules, and logic that handle personal data. Processes should also be established for receiving information on vulnerabilities from external sources related to systems that contain privacy data. These vulnerabilities can have an outsized impact if exploited, or if made public, and accordingly these vulnerabilities may need to be placed toward the top end of the remediation queue.

Third-party components are a necessary commodity in modern software engineering and design. While these components are often necessary, third-party components handling PII should be given extra attention, inventoried, and validated accordingly. Be sure to regularly monitor publicly released vulnerabilities reported for these companies and the software they use within their technology stack. Many third-party components are not meant to be connected to the internet. Applications and other components that do not require network access should be placed within a private network that lacks external access.

Threat modeling activities are useful exercises in understanding how external and internal threat actors may attempt to steal personal data. These modeling activities should explicitly take into account personal data, with focused reviews for personal datastores and other applications that access PII.

Many enterprises have privacy policies on their websites and customer facing applications. These policies define what information is collected, how it's used and shared, and how it's protected. Consider posting a privacy policy for internal business applications. This is true for traditional operating system-based applications, alongside mobile and web-based applications.

Fair Information Practice Principles

- **The Collection Limitation Principle.** Third-party software libraries, components, APIs, and external software developers should not collect PII and other personal data unless explicitly required.
- **The Data Quality Principle.** PII and other personal data collected by third-party software libraries, components, APIs, and external software developers should only be used for the business process they were designed for.
- **The Purpose Specification Principle.** Employees should be informed of what information will be collected by third-party software libraries, components, APIs, and external software developers and how the information will be used.
- **The Use Limitation Principle.** Employees should be informed if data collected by third-party software libraries, components, APIs, and external software developers will be transferred to other systems owned by third-party service providers.
- **The Security Safeguards Principle.** Care should be taken to secure any data that likely includes PII and other personal data.
- **The Openness Principle.** Employees with PII and other personal data collected by enterprise systems should understand what external systems may contain their personal data.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be collected by third-party software libraries, components, APIs, and external software developers. A lawful basis is needed for collecting personal data.
- **Purpose limitation.** Third-party software libraries, components, APIs, and external software developers should not be intentionally configured with the ability to collect PII and other personal data. Users should be informed in writing when their data is to be shared.
- **Data minimization.** Personal data should not be collected unless it is necessary. Written processes should be in place to avoid undesirable personal data collection.

- **Accuracy of data.** Any personal data should be maintained with written processes documented for how user data is maintained and how incorrect data can be corrected or, more likely, removed.
- **Storage limitation.** User data should only be stored for as long as needed, if it is needed at all. Obsolete or unnecessary user data should be deleted without delay.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Control 3: Data Protection for protecting this information. Personal data should be protected from unauthorized access, modification, and disclosure and can be leveraged by an attacker to obtain unauthorized access to an enterprise's systems.

Control 16 Privacy Applicability Table

CIS Control 16: Application Software Security				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
16.1	Applications	Protect	**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.	**Yes** Software engineers should be trained on handling PII and other personal data and how to include privacy considerations in the design of their software.
16.2	Applications	Protect	**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.	**Yes** IT systems handling PII and other personal data may need to have their vulnerabilities prioritized over others. It may be wise to carve out a specific section of this process to address privacy vulnerabilities.
16.3	Applications	Protect	**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 creates vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.	**No** Although an important activity, there is no direct privacy impact.

CIS Control 16: Application Software Security				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
16.4	Applications	Protect	**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 the component is still supported.	**Yes** Any third-party component handling personal data should be afforded additional scrutiny, inventoried, and validated accordingly.
16.5	Applications	Protect	**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.	**No** There are no privacy specific aspects of keeping third-party components up-to-date.
16.6	Applications	Protect	**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.	**Yes** IT systems handling PII and other personal data may need to have their vulnerabilities prioritized over others.
16.7	Applications	Protect	**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.	**No** This should be performed for all application infrastructure, regardless of the types of data stored within.
16.8	Applications	Protect	**Separate Production and Non-Production Systems** Maintain separate environments for production and non-production systems.	**No** Although an important Safeguard, there are no privacy specific impacts.
16.9	Applications	Protect	**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.	**No** This should happen for all developers. No privacy impact. This is an opportunity to train developers on the core concepts of privacy engineering.

CIS Control 16: Application Software Security				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
16.10	Applications	Protect	**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.	**No** This should happen for all developers. No privacy impact. This is an opportunity to train developers on the core concepts of privacy engineering.
16.11	Applications	Protect	**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.	**No** Vetted modules and services should be leveraged regardless of data type. There is no privacy impact.
16.12	Applications	Protect	**Implement Code-Level Security Checks** Apply static and dynamic analysis tools within the application lifecycle to verify that secure coding practices are being followed.	**No** There are no privacy impacts within code-level security checks.
16.13	Applications	Protect	**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.	**Yes** There is often a resource component to penetration testing, and certain systems receive more testing than others. Systems containing PII and other personal data should receive additional scrutiny from penetration testers.
16.14	Applications	Protect	**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.	**Yes** Threat modeling activities should include additional and focused review for private datastores and other applications that access that data.

CONTROL 17

Incident Response Management

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.

Privacy Applicability

This Control assists enterprises in planning for, and responding to, a cyber incident. Two aspects of privacy exist within this Control. The first is how to respond to a privacy incident, such as the unauthorized access or disclosure of personal or sensitive information. The second is how to maintain privacy for all individuals when responding to a cyber incident.

Privacy Implications

- Incident response teams are often composed of internal stakeholders, internal and external technical experts, and legal staff. Throughout the course of their response duties, members of incident response teams may have access to personal data. For instance, when reviewing logs to understand the manner and date of unauthorized access and reviewing leaked databases to confirm the data's origin, response team members are likely to view personal data. They may intentionally abuse or improperly handle their access to this information
- Cyber incidents often have a privacy component due to what enterprise resources were accessed, or what data was exfiltrated. This often brings local and federal privacy law into account. These laws may have specific mechanisms and timeframes for notifying the government and affected entities of a cybersecurity incident or data breach. Enterprises that do not appropriately notify may face fines or other legal action.
- Data breaches affecting PII need to be reported to the appropriate entities within pre-specified reporting timeframes.

Data Collection

Incident response team members will collect information from various systems across the enterprise network as they perform their duties to understand the manner and scope of an intrusion. Legal counsel may also obtain access to this data. It may be prudent to redact certain portions of information and obtain a nondisclosure agreement before providing this information to other entities.

Data Storage

All data collected during incident response activities needs to be protected as it is often personal data, but also may be needed for upcoming legal proceedings. Collected information may be stored outside of the primary enterprise, within a third-party incident response enterprise's management platform. It is important to protect forensic data, and access to this data, similar to other privacy data.

Additional Discussion

Data breach reporting requirements should also be built into incident response plans. Enterprises need to establish a process for responding to cyber incidents with a privacy component. This may take the form of distinct processes when dealing with a data breach. Using an external legal team to oversee incidents is often considered a best practice, as incident reports can be marked as "attorney client privileged." Additionally, specific individuals should be assigned for analyzing PII and other sensitive information throughout the lifecycle of the breach investigation. Descriptions of incident response and forensic procedures should be disclosed, so that employees are aware. Incident response procedures dealing with privacy breaches should be regularly exercised.

Fair Information Practice Principles

- **The Collection Limitation Principle.** Incident response team members should not collect PII and other personal data unless explicitly required.
- **The Data Quality Principle.** PII and other personal data collected by incident response team members should only be used for incident response activities.
- **The Purpose Specification Principle.** Employees should be informed what information will be collected by an incident response team and how the information will be used.
- **The Use Limitation Principle.** Employees should be informed if data collected by incident response team members will be transferred to other systems owned by third-party service providers.
- **The Security Safeguards Principle.** Care should be taken to secure any data that likely includes PII and other personal data.
- **The Openness Principle.** Employees with PII and other personal data collected by an incident response team should understand what external systems may contain their personal data.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be collected by incident response personnel. A lawful basis is needed for collecting personal data.
- **Purpose limitation.** PII and other personal data collected by incident response team members should only be used for incident response activities. Users should be informed in writing when their data is to be shared.
- **Data minimization.** Personal data should not be collected unless it is necessary during the course of a response. Written processes should be in place to avoid undesirable personal data collection, since the incident response process is often fast-paced.
- **Accuracy of data.** Any personal data should be maintained with written processes documented for how user data is maintained and how incorrect data can be corrected or, more likely, removed. This is very applicable to incident response as situations change rapidly and the incident response team may collect more information than is strictly necessary. Reviewing the collected information and deleting unnecessary information is a common practice.
- **Storage limitation.** User data should only be stored for as long as needed, if it is needed at all. Obsolete or unnecessary user data should be deleted without delay.

- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Control 3: Data Protection for protecting this information. Personal data collected during the incident response process should be protected from unauthorized access, modification, and disclosure and can be leveraged by an attacker to obtain unauthorized access to an enterprise's systems.

Control 17 Privacy Applicability Table

CIS Control 17: Incident Response Management				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
17.1		Respond	**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.	**Yes** Personnel designated to handle incidents should be trained on handling PII and other personal data. They should understand applicable regulatory requirements facing the enterprise.
17.2		Respond	**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.	**Yes** Contact information for responders should not be overly granular and contain only the required PII.
17.3		Respond	**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.	**Yes** This process should closely follow local and national laws. Timeframes of notification, and who to notify, can be different based on region. Failure to appropriately notify affected parties can result in penalties against the enterprise.
17.4		Respond	**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.	**Yes** A process for responding to a privacy incident should be established. This may take the form of special instructions when dealing with a broader cyber incident.
17.5		Respond	**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.	**Yes** Someone should be assigned for tracking the processing of PII and other private information. There should also be someone designated for ensuring compliance with local regulatory and compliance requirements in regards to privacy.

CIS Control 17: Incident Response Management				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
17.6		Respond	**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.	**Yes** Any communication methods should meet any regulatory or compliance requirements for privacy breaches.
17.7		Recover	**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.	**Yes** Incident response procedures dealing with privacy breaches should be regularly exercised.
17.8		Recover	**Conduct Post-Incident Reviews** Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.	**Yes** Post-incident reviews should be conducted for all cyber incidents that involve PII and other personal data.
17.9		Recover	**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.	**Yes** Security event thresholds should be established for cyber incidents that involve PII and other personal data.

CONTROL 18

Penetration Testing

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.

Privacy Applicability

This Control focuses on how to effectively simulate the actions of an external and/or internal attacker within an enterprise environment. This may include exploiting a weakness or vulnerability in a system or network. Many of the Safeguards within this Control contain privacy impacts that can be at least mitigated via policy and clearly written agreements before any testing is performed. All of this Control's Safeguards apply.

Privacy Implications

- As part of the testing process, personal information may be obtained by the penetration testers. This is especially true for penetration testing with a social component and those looking to include BYOD mobile devices.
- Improper handling or disposal of PII and other personal data obtained throughout the course of a testing engagement.

Data Collection

Any data collected by penetration testers throughout the course of their engagement should be well secured. Both organizations should agree on data disposal techniques.

Data Storage

Data obtained by penetration testers should not be shared, and penetration testers should quickly notify the enterprise.

Additional Discussion

The development of a penetration testing program should take the privacy of employees and users into account during formation. Since modern penetration testing engagements will often contain a social component, acceptable rules for gathering information from the web should be established. This could include collection of highly personal information about specific targets for phishing campaigns, to include publicly available information from social networks, public records, and news sites.

A penetration testing program should also address what level of access and knowledge external penetration testers receive. This is especially true for systems that contain PII and other personal data. Members of any external or contracted penetration testing team should be treated as third-party service providers, and Control 15 should be applied. Finally, how to handle mobile devices and data should be scoped appropriately into the penetration testing program. This should include how to handle any BYOD devices.

Fair Information Practice Principles

- **The Collection Limitation Principle.** Penetration testing should not collect PII and other personal data unless explicitly required in pre-approved testing methodologies.
- **The Data Quality Principle.** PII and other personal data collected by penetration testers should only be used for testing engagement.
- **The Purpose Specification Principle.** Employees should be informed what information could be collected by penetration testers and how the information will be used.
- **The Use Limitation Principle.** Employees should be informed if data collected by penetration testers will be transferred to other systems owned by third-party service providers. This includes if any penetration testing tools or frameworks will also collect PII and other personal data.
- **The Security Safeguards Principle.** Care should be taken to secure any data that likely includes PII and other personal data.
- **The Openness Principle.** Employees with PII and other personal data collected by penetration testers should understand what external systems may contain their personal data.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees should have the ability to reasonably request to see what data is stored about them.
- **The Accountability Principle.** It will be uncommon to find service providers who comply with many of the FIPPs.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees should have the opportunity to make an informed decision on the type of personal data that will be collected by penetration testers. A lawful basis is needed for collecting personal data.
- **Purpose limitation.** PII and other personal data collected by penetration testers should only be used for related activities. Users should be informed in writing when their data is to be shared. Generally, penetration testers should be told not to access personal information, and this should be documented within any rules of engagement beforehand.
- **Data minimization.** Personal data should not be collected unless it is necessary during the course of a testing engagement. Written processes should be in place to avoid undesirable personal data collection, but sometimes personal data will be exposed during a penetration testing engagement.
- **Accuracy of data.** Any personal data should be maintained with written processes documented for how user data is maintained and how incorrect data can be corrected or, more likely, removed. This is very applicable to penetration testing since personal data will sometimes be exposed during a penetration testing engagement. Reviewing the collected information and deleting unnecessary information is a common practice.
- **Storage limitation.** User data should only be stored for as long as needed, if it is needed at all. Obsolete or unnecessary user data should be deleted without delay.
- **Integrity and confidentiality.** The CIS Controls can be leveraged to enable this principle, such as Control 3: Data Protection for protecting this information. Personal data collected during a testing engagement should be protected from unauthorized access, modification, and disclosure and can be leveraged by an attacker to obtain unauthorized access to an enterprise's systems.

Control 18 Privacy Applicability Table

CIS Control 18: Penetration Testing				
Safeguard	Asset Type	Security Function	Control Title/ Description	Applicability Included? Applicability Justification and Privacy Considerations
18.1		Identify	**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.	**Yes** The development of this program should take the privacy of employees and users into account during formation.
18.2	Network	Identify	**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.	**Yes** External penetration testers should be made aware of systems that contain personal data in order to ensure those systems are not included within the scope of the testing engagement unless that is intended.
18.3	Network	Protect	**Remediate Penetration Test Findings** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.	**Yes** Penetration testing finds in systems containing PII and other personal data should be prioritized for remediation.
18.4	Network	Protect	**Validate Security Measures** Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.	**Yes** Security measures for systems storing PII and other personal data should be validated earlier than others, although this is obviously a business decision.
18.5		Identify	**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.	**Yes** Internal tests should abide by the rules of engagement for dealing with systems containing PII and personal data.

Acronyms and Abbreviations

AAA	Authentication, Authorization and Accounting
API	Application Programming Interface
BYOD	Bring Your Own Device
CIPP	Certified Information Privacy Professional
CIS	Center for Internet Security
COPE	Corporate Owned, Personally Enabled
CSP	Cloud Service Providers
DLP	Data Loss Protection
DHCP	Dynamic Host Configuration Protocol
DMARC	Domain-based Message Authentication, Reporting & Conformance
DNS	Domain Name System
EMM	Enterprise Mobility Management
ETSI	European Telecommunications Standards Institute
EU	European Union
FIPPs	Fair Information Practice Principles
GDPR	General Data Protection Regulation
HR	Human Resource
HTTPS	Hypertext Transfer Protocol Secure
IAPP	International Association Privacy Professionals
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
MAC	Media Access Control (address)
NAS	National Academy of Sciences
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SME	Small/Medium Enterprise
SSID	Service Set Identifier
SSO	Single Sign-On
URL	Uniform Resource Locator
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

Links and Resources

- CIS Controls: https://www.cisecurity.org/controls/
- CIS Controls Cloud Companion Guide: https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/
- CIS Controls Mobile Companion Guide: https://www.cisecurity.org/white-papers/cis-controls-mobile-companion-guide-2/
- Fair Information Practice Principles (FIPPs): https://iapp.org/resources/article/fair-information-practices
- General Data Protection Regulation (GDPR): https://ec.europa.eu/info/law/law-topic/data-protection_en
- National Academies of Sciences: Privacy Research and Best Practices: Summary of a Workshop for the Intelligence Community: https://www.dni.gov/files/documents/CLPO/NAP%20Privacy%20Research%20and%20Best%20Practices.pdf
- How To Do A Privacy Impact Assessment (PIA): Privacy-Impact-Assessment-Part-2-FA.pdf
- National Institute of Standards & Technology Privacy Framework: https://www.nist.gov/privacy-framework
- European Telecommunications Standards Institute (ETSI) Critical Security Controls for Effective Cyber Defence [sic]; Part 5: Privacy enhancement: https://www.etsi.org/deliver/etsi_tr/103300_103399/10330505/01.01.01_60/tr_10330505v010101p.pdf
- Department of Homeland Security Privacy Training & Awareness: https://www.dhs.gov/privacy-training
- US Nuclear Regulatory Commission Privacy Program: https://www.nrc.gov/privacy/index.html
- California Department of Aging: Privacy & Information Security Awareness Training: https://www.aging.ca.gov/Information_Security/Privacy_and_Information_Security_Awareness_Training

Closing Notes

In this document, we provide guidance on how to apply privacy best practices while implementing the CIS Controls Version 8. The newest version of the CIS Controls and other complementary documents may be found at www.cisecurity.org.

As a nonprofit organization driven by its volunteers, we are always in the process of looking for new topics and assistance in creating cybersecurity guidance. If you are interested in volunteering and/or have questions, comments, or have identified ways to improve this guide, please write us at: controlsinfo@cisecurity.org.

All references to tools or other products in this document are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Contact Information

Center for Internet Security
31 Tech Valley Drive
East Greenbush, N.Y. 12061
518.266.3460
controlsinfo@cisecurity.org

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 Critical Security 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. election offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

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