ETSI TR 103 305-5 V2.1.1 (2023-02)

Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Privacy and personal data protection enhancement

Reference

RTR/CYBER-0075

Keywords

cyber security, cyber-defence, information assurance, privacy

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 5 of a multi-part deliverable covering the Critical Security Controls for Effective Cyber Defence. Full details of the entire series can be found in part 1 [i.2].

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document is an evolving repository for privacy and personal data protection enhancement guidelines for Critical Security Control implementations. These guidelines include a privacy impact assessment mechanism as well as implementations aiming to meet provisions of the EU General Data Protection Regulation (GDPR) using the Critical Security Controls in furthering data protection objectives [i.1] and [i.11].

Introduction

The Critical Security 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 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 Controls come from a wide range of sectors, including retail, manufacturing, healthcare, transport, education, government, defense, and others. While the Controls address the general practices that most organizations should take to secure their systems, some operational environments and aspects of an information security program can present unique requirements not addressed by the Controls.

The GDPR [i.1] uses the term "data protection" rather than privacy, but furthers the EU Directive on privacy and personal data protection without imposing additional obligations [i.11]. The purpose of the present document is to develop best practices and guidance for implementing the Controls that further data protection while carefully considering the privacy impacts an organization can have on its workforce, customers, and third parties. It supports the objectives of the Controls by aligning data protection and privacy principles and highlighting potential concerns that can arise through the usage of the Controls.

1 Scope

The present document is an evolving repository for data protection and privacy enhancing implementations using the Critical Security Controls, ETSI TR 103 305-1 [i.2]. These presently include a comprehensive, consistent approach for analysing the latest version of the Controls aiming to meet requirements that include the EU General Data Protection Regulation (GDPR) [i.1] and the U.S. DHS Fair Information Practice Principles [i.4].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)).

[i.2] ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.3] ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.4] U.S. Department of Homeland Security (DHS): "Fair Information Practice Principles (FIPPs)".

NOTE: See also https://iapp.org/resources/article/fair-information-practices/.

[i.5] New Zealand Privacy Commissioner: "Privacy Impact Assessment Toolkit".

[i.6] NIST: "Privacy Framework".

[i.7] Commission Nationale de l'Informatique et des Libertés (CNIL): "GDPR Toolkit".

[i.8] ico (Information Commissioner's Office): "Data protection impact assessments".

[i.9] ISO/IEC 29134:2017: "Information technology -- Security techniques -- Guidelines for privacy impact assessment".

[i.10] ISO/IEC 27701:2019: "Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines".

[i.11] Consolidated text: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[i.12] CCS '18: "Mystique: Uncovering Information Leakage from Browser Extensions".

[i.13] CIS: Controls Cloud Companion Guide, version 8.

[i.14] CIS: Critical Security Controls® Mobile Companion Guide, version 8.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in Directive 2002/58/EC [i.11], Regulation (EU) 2016/679 [i.1] and the following apply:

end-user: user of an electronic communication service or product

privacy: user right to certain controls on processing, movement and protection of personal data

NOTE: As defined in Directive 2002/58/EC [i.11].

user: any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service

NOTE: As defined in Directive 2002/58/EC [i.11].

username: identifier associated with an end-user used for accessing a service or product

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
API	Application Programming Interface
BYOD	Bring Your Own Device
CIS	Center for Internet Security
CNIL	Commission Nationale de l'Informatique et des Libertés
COPE	Corporate Owned, Personally Enabled
CSP	Cloud Service Providers
CVSS	Common Vulnerability Scoring System
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DLP	Data Loss Protection
DMARC	Domain-based Message Authentication, Reporting & Conformance
DNS	Domain Name System
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EMM	Enterprise Mobility Management
EU	European Union
FIPP	Fair Information Practice Principles
GDPR	General Data Protection Regulation
GSM	Global System for Mobile
HR	Human Resource
HTTPS	Hypertext Transfer Protocol Secure
IAPP	International Association of Privacy Professionals
ICO	Information Commissioner's Office (UK)
ICS	Industrial Control Systems
ICS-ISAC	Industrial Control Systems Information Sharing and Analysis Center

IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IG1	Implementation Group 1
IG2	Implementation Group 2
IG3	Implementation Group 3
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing & Analysis Center
IT	Information Technology
LTE	Long-Term Evolution
MAC	Media Access Control (address)
MFA	Multifactor Authentication
N/A	Not Applicable
NAS	National Academy of Sciences
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SEIM	Security Event and Incident Management
SIEM	Security Information and Event Management
SIG	Special Interest Group
SLA	Service Level Agreement
SP	Special Publication
SSID	Service Set Identifier
SSO	Single Sign-On
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

4 Critical Security Controls: Privacy Assessment Methodology

4.1 Methodology

A consistent approach is needed for analyzing the Controls in the context of privacy. The Fair Information Practice Principles (FIPPs) [i.4] and the General Data Protection Regulation (GDPR) [i.1] are being leveraged to help analyse the privacy implications of each Control [i.2]. The application of the principles can differ among national and business jurisdictions.

The FIPPs are directly quoted as follows:

- ***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.*

- ***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.*

- ***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.*

- ***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.*

- ***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.*

- ***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.*

- ***The Individual Participation Principle.*** *An individual should have the right:*

    - *to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;*

    - *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;*

    - *to be given reasons if a request made under subparagraphs (a) and (b) is denied and to be able to challenge such denial; and*

    - *to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended;*

- ***The Accountability Principle.*** *A data controller should be accountable for complying with measures which give effect to the principles stated above*."

The GDPR [i.1] is a multifaceted regulation governing the processing of personal data, as well as other technical aspects of an enterprise, in the European Union and beyond. The essential characteristics of the regulation are to protect personal data as a fundamental right. Many new personal data protection regulations across the world are using the GDPR as framework in their own country, state, or region. The GDPR provisions apply to any enterprise that processes the personal data of EU citizens. Therefore, each Control is analysed for steps enterprises need to take in order to ensure that they are including GDPR principles in their business. Implementation of the GDPR is furthered through the European Data Protection Board (EDPB) and its secretariat provided by the European Data Protection Supervisor (EDPS).

The requirements of the GDPR [i.1] covered by the present document include the following principles:

- ***"Lawfulness, fairness, and transparency:*** *processed lawfully, fairly and in a transparent manner in relation to the data subject*

- ***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*

- ***Data minimization:*** *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*

- ***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*

- ***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 measures required by this Regulation in order to safeguard the rights and freedoms of the data subject*

- ***Integrity & Confidentiality:*** *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"*

These are principles of the GDPR. It also declares a number of rights for users. This includes the right to erasure ('right to be forgotten'), which allows a user to request that their data be deleted from a data controller 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, companies subject to GDPR [i.1] are required to comply with an array of process and privacy by design provisions including notification to competent supervisory authorities and the data subject if the company suffers a data breach that places personal data at high risk.

In addition to the FIPPs and the GDPR principles, for each of the 18 Controls, the following information is provided in the present document:

- **Privacy Applicability.** Explores the degree to which a Control pertains to privacy. Only specific Safeguards within a Control contribute towards privacy. This could include protecting the privacy of employees and customers, but can also include of the organization's IT systems.
- **Privacy Implications.** Includes the privacy issues and/or risks associated with implementing a specific Control. This helps implement the Use Limitation, Security, and Accountability FIPPs.
- **Data Collection.** This focuses on the types of data collected by the enterprise when implementing a Control. While there is always a specific focus on personally identifiable information (PII), other data types can 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 is stored somewhere until it is deleted. This portion analyses issues associated with storing data such as where and how data is stored. This also includes the parties involved in the storage process.
- **Privacy 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 FIPPs.
- **Fair Information Practice Principles.** Concerns and other information associated with the FIPPs Principles.
- **General Data Protection Principles.** Concerns and other information associated with the GDPR Principles.

4.2 Limitations

While a complete treatment of privacy could be quite lengthy, the present document 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 are not included, enterprises should be mindful of the following issues, where applicable:

- Evolving national and international privacy laws.
- Breach disclosure requirements that are locally, regionally, or nationally applicable. This also includes 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 as users.
- Data portability requirements.
- International transfers.

A Control Applicability Table is provided at the end of each clause 5, and indicates the applicability of each Safeguard to privacy. The letter "Y" indicates that a Safeguard has privacy impacts, and "N" indicates there is no privacy impact. These tables note privacy impacts that a particular Safeguard may have, and can assist in privacy engineering efforts. However, it is sometimes unclear when a Safeguard is directly applicable to privacy. For example, many Safeguards are designed to keep information secure from unauthorized disclosure by using cryptography and access control.

Ultimately, all of the Safeguards are applicable because they are designed to secure the IT systems which hold the personal data.

In noting privacy implications of the Controls and suggesting mitigations, the present 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 users from having their passwords posted online.

4.3 Privacy Assessments

There are many ways to assess how privacy is protected within an enterprise. The U.S. National Academy of Sciences (NAS) Privacy Research and Best Practices report 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"*. Enterprises are encouraged 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. New Zealand, France and the UK have published tools and guidelines for assessing data protection and privacy impacts, see [i.5], [i.7], [i.8]. In addition, the ISO/IEC have published similar material in ISO/IEC 29134 [i.9] and ISO/IEC 27701 [i.10].

The U.S. National Institute of Standards and Technology (NIST) also provides a Privacy Framework that is a more recent approach for assessing privacy within an enterprise [i.6]. The Framework is a "*tool that can help an enterprise create or improve a privacy program. Effective privacy risk management can help build trust in products and services, communicate better about the privacy practices, and meet the 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, ETSI has provided resources for privacy enhancing implementations using the Controls via the present document. There are a variety of mechanisms within the present document that can facilitate and encourage privacy protection. In addition, the Controls can help meet provisions of the EU General Data Protection Regulation (GDPR) [i.1] using the Critical Security Controls. The present document is directed at both achieving privacy objectives and performing privacy impact assessments.

The Controls do not contain a Control specifically focusing on privacy. There is no single approach for performing a privacy assessment. Instead, multiple approaches are provided to make users aware of the options that exist to facilitate increasing privacy mechanisms within an organization.

5 Critical Security Controls: Privacy Assessment

5.1 Control 1: Inventory and Control of Enterprise Assets

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

Privacy Applicability

This Control is applicable to the creation and maintenance of device inventories. Privacy principles should be incorporated into the device inventory process, both from a technological and procedural standpoint. A majority of the Safeguards within this Control are not 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 individuals' name or identifier, which explicit 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.

- It is common for enterprises to provision device models to employees based on their role within the enterprise. For instance, developers can be provisioned with more powerful laptops than general staff, or executives can receive tablets. Knowledge of this information could allow inference of the user's role in the organization 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 can also track device usage, and even the contents, which is likely to involve personal data.

Data Collection

Common data types collected for this Control will include information about the device, such as model, owner, IP, and device name. Device name can 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 can be stored in a spreadsheet located on a system administrator's system. The inventory can 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 can be stored locally but can also be stored in a cloud-based system outside of the enterprise's control. The external service provider can 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 and hardware providing data redundancy can 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 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 Controls and Safeguards since they contain personal information 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 and other data subjects 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 Controls can be leveraged to enable this Principle, such as Control 3: Data Protection.

- **The Openness Principle.** Employees and other data subjects should understand what external systems can contain personal data and why.

- **The Individual Participation Principle.** Employees and other data subjects should have the ability to reasonably request to see what data is held about them in the inventory

- **The Accountability Principle.** This principle should be discussed with the service provider before selection and usage.

General Data Protection Regulation Principles

- **Lawfulness, fairness, and transparency.** Employees and other data subjects should understand what personal data will be kept within the enterprise asset inventory, and how it will be used. A lawful basis is

- **Purpose limitation.** Users should be informed in writing about the 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 can conflict with the need to leverage asset inventory data for secure baselines and vulnerability management. This may only apply to personally owned devices. Organization owned devices need 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 should 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 & Confidentiality.** The 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: Inventory and Control of Enterprise Assets					Implementation Groups			Applicability	
Safe guard	**Asset Type**	**Security Function**	**Control Title**	**Control Descriptions**	**IG1**	**IG2**	**IG3**	**Included?**	**Applicability Justification & Privacy Considerations**
1.1	Devices	Identity	Establish and Maintain Detailed Enterprise Asset Inventory	See [i.2]	●	●	●	Y	The information collected within asset inventories likely contains, or is directly connected to, information systems containing PII and other personal data. Make sure the organization has, and implements, a data handling policy for the inventory that applies the principles (above).
1.2	Devices	Respond	Address Unauthorized Assets	See [i.2]	●	●	●	Y	Identifying and addressing unauthorized assets can intentionally or unintentionally involve the collection of personal data (e.g. the names of commonly used Wi-Fi 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).
1.3	Devices	Detect	Utilize an Active Discovery Tool	See [i.2]		●	●	Y	Using automated tools to interrogate devices can obtain information that the organization can 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	See [i.2]		●	●	Y	DHCP logs contain sensitive information because it maps device identifiers to an IP address, so it is critical that an organization limits 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	See [i.2]			●	Y	Passive discovery can involve the collection and use of device identifiers that are unique (e.g. hostnames, MAC addresses and IP addresses). The organization 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 can be personal data. Even the identifiers, when linked or able to be linked to an individual, can be considered personal data.

5.2 Control 2: Inventory and Control of Software Assets

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

Privacy Applicability

This Control is applicable to the development and maintenance of software inventories. Privacy principles should be incorporated into the software inventory process, both from a technological and 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 and other data subjects, 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 can 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 and other data subjects.

Data Collection

Common forms of data collected for this Control will include information about the device including model, owner, IP, and device name. Device name can 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 can be stored in a 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 can be stored locally but can also be stored in a cloud-based system outside of the enterprise's control. The service provider can have access to all data inventory information. Any hot sites or other organizations providing data redundancy can 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 and other data subjects 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 forpurposes, 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 data protection.

- **The Openness Principle**. Employees and other data subjects should understand what external systems can contain personal data.

- **The Individual Participation Principle**. Employees and other data subjects should have the ability to reasonably request to see what data is held about them in the inventory.

- **The Accountability Principle**. This principle should be discussed with the service provider before selection and usage.

General Data Protection Regulation Principles:

- **Lawfulness, fairness, and transparency**. Employees and other data subjects 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 the 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 can conflict with the need to leverage software inventory data for secure baselines and vulnerability management. This may only apply to personally owned devices. Organization owned devices need 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 should 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 & Confidentiality.** The 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: Inventory and Control of Software Assets					Imple-mentation Groups			Applicability	
Safe guard	Asset Type	Security Function	Control Title	Control Descriptions	IG 1	IG 2	IG 3	Included?	Applicability Justification & Privacy Considerations
2.1	Applications	Identify	Establish and Maintain a Software Inventory	See [i.2]	●	●	●	Y	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	See [i.2]	●	●	●	N	Ensuring software assets are supported does not present privacy impacts.
2.3	Applications	Respond	Address Unauthorized Software	See [i.2]	●	●	●	N	Removing unauthorized applications does not present privacy impacts.
2.4	Applications	Detect	Utilize Automated Software Inventory Tools	See [i.2]		●	●	Y	Using automated tools to actively identify installed applications will likely provide personal information to the employer, especially on mobile platforms. This can include apps related to lifestyle, health tracking, or personal finances.
2.5	Applications	Protect	Allowlist Authorized Software	See [i.2]		●	●	Y	Allowlisting software on personal mobile devices can be privacy invasive based on the mobile operating system and specific implementation.
2.6	Applications	Protect	Allowlist Authorized Libraries	See [i.2]		●	●	N	This specific type of allowlisting does not present privacy impacts.
2.7	Applications	Protect	Allowlist Authorized Scripts	See [i.2]			●	N	This specific type of allowlisting does not present privacy impacts.

5.3 Control 3: Data Protection

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

Privacy Applicability

Data Protection is a 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 the present document's scope, keeping information safe from unauthorized disclosure is not the only consideration for being applicable to privacy. If it was the only consideration, then all of the Safeguards within the 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 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 expenditure.

- Implementing many of the Safeguards within this Control can protect PII and other personal data. Yet these same systems can 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 private data.

Safeguard 3.13 - Deploy a Data Loss Prevention Solution can be leveraged in an automated fashion to identify collected PII and other personal data in the enterprise. DLP usage can reveal unknown PII, 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 private information. 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 private information stored there should be explicitly understood and approved. See the Cloud Companion Guide for how to secure Cloud-based systems [i.13].

Disposal of stored private information (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 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, including a data inventory classification scheme could be interpreted in a manner to enhance privacy. These three 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 protection.

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 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.** PII and other 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.

- **The Purpose Specification Principle.** Employees and other data subjects 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 or required within the jurisdiction.

- **The Security Safeguards Principle.** Control 3, and the 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 can contain personal data.

- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees and other data subjects 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 and other data subjects 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 the 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 and protected. This can conflict with the need to leverage software inventory data for secure baselines and vulnerability management. This may only apply to personally owned devices. Organization owned devices need not be subject to this principle.

- **Data minimization.** Unnecessary personal and customer data should not be collected or maintained unless it is specifically needed. The data that is collected should be specifically used for its original intended purpose. Employees and other data subjects 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 data inventory 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 & Confidentiality.** The 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: Data Protection					Imple-mentation Groups			Applicability	
Safeguard	**Asset Type**	**Security Function**	**Control Title**	**Control Descriptions**	**IG1**	**IG2**	**IG3**	**Included?**	**Applicability Justification & Privacy Considerations**
3.1	Data	Identify	Establish and Maintain a Data Management Process	See [i.2]	●	●	●	Y	This can be leveraged to manage PII and other types of private information.
3.2	Data	Identify	Establish and Maintain a Data Inventory	See [i.2]	●	●	●	Y	This can be leveraged to manage PII and other types of private information.
3.3	Data	Protect	Configure Data Access Control Lists	See [i.2]	●	●	●	Y	Only certain users and roles should be provided access to certain types of protected and private information.
3.4	Data	Protect	Enforce Data Retention	See [i.2]	●	●	●	Y	The privacy implications associated with retained data should be analysed and understood.
3.5	Data	Protect	Securely Dispose of Data	See [i.2]	●	●	●	Y	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	See [i.2]	●	●	●	Y	This helps protect stored information that is private.
3.7	Data	Identify	Establish and Maintain a Data Classification Scheme	See [i.2]		●	●	Y	This can be leveraged to manage PII and other types of private information.
3.8	Data	Identify	Document Data Flows	See [i.2]		●	●	Y	This can ensure an enterprise knows where private information is likely to be sent.
3.9	Data	Protect	Encrypt Data on Removable Media	See [i.2]		●	●	Y	This helps protect stored information that is private.
3.10	Data	Protect	Encrypt Sensitive Data in Transit	See [i.2]		●	●	Y	This helps protect stored information that is private.
3.11	Data	Protect	Encrypt Sensitive Data At Rest	See [i.2]		●	●	Y	This helps protect stored information that is private.
3.12	Network	Protect	Segment Data Processing and Storage Based on Sensitivity	See [i.2]		●	●	Y	Private information should only be stored in approved locations and on appropriate systems.
3.13	Data	Protect	Deploy a Data Loss Prevention Solution	See [i.2]			●	Y	This can be helpful to identify PII and other private information stored within the enterprise, or leaving in an unauthorized manner.
3.14	Data	Detect	Log Sensitive Data Access	See [i.2]			●	Y	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.

5.4 Control 4: Secure Configuration for Enterprise Assets and Software

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

Privacy Applicability

Secure configurations for hardware and software assets can help enable privacy for employees by preventing data breaches. Certain configuration settings in popular products can be viewed as outright vulnerabilities, whereas other settings can 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 can cause data to be collected, such as traffic logs or data access logs. Because this information can be sensitive, IT should understand the settings they are enabling so that this information is not 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 should 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 private 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 private data outside the enterprise. As few parties as possible, if any, should have access to the employee information.

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. Yet 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 organizational 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). See the Mobile Companion Guide [i.14].

Fair Information Practice Principles:

- **The Collection Limitation Principle.** It is common for employees to be notified that they are being tracked in the US via IT policies. 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 or required in the jurisdiction. This includes providing network data to other service providers.
- **The Security Safeguards Principle.** Care should be taken to carefully 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 can contain their personal data.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees and other data subjects 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 and other data subjects 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 the purpose for collecting.
- **Data minimization.** Unnecessary personal and customer data should not be collected or maintained unless it is specifically needed. The data that is collected should be specifically used for its original intended purpose. Employees and other data subjects 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 data inventory 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 & Confidentiality.** The 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 help fulfill the provisions of Article 32 of GDPR titled *Security of processing*. Article 32 1(a) includes " the pseudonymisation and encryption of personal data" as measure. Safeguards 3.6, 3.9, 3.10, and 3.11 can help to accomplish this task.

Control 4: Secure Configuration of Enterprise Assets and Software					Imple-mentation Groups			Applicability	
Safeguard	**Asset Type**	**Security Function**	**Control Title**	**Control Descriptions**	**IG1**	**IG2**	**IG3**	**Included?**	**Applicability Justification & Privacy Considerations**
4.1	Applications	Protect	Establish and Maintain a Secure Configuration Process	See [i.2]	●	●	●	Y	Secure configuration processes should take privacy into account when deciding upon configurations. This should include what data is generated, and where it is stored. Also 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	See [i.2]	●	●	●	Y	Privacy should be taken into account 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	See [i.2]	●	●	●	N	This helps prevent naive attempts to access unauthorized private data, but there are no privacy impacts.
4.4	Devices	Protect	Implement and Manage a Firewall on Servers	See [i.2]	●	●	●	Y	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 user traffic.
4.5	Devices	Protect	Implement and Manage a Firewall on End-User Devices	See [i.2]	●	●	●	Y	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	See [i.2]	●	●	●	Y	System administrators will at times have to access PII and other sensitive data. Using secure protocols to do so prevents eavesdropping and other attacks over the wire. Yet system administrators should be trained on acceptable activities and violations of user privacy when acting as administrator.
4.7	Users	Protect	Manage Default Accounts on Enterprise Assets and Software	See [i.2]	●	●	●	Y	Certain accounts on systems will be given additional privileges and can access sensitive information. Access to these accounts needs to be properly managed, with users of those accounts properly trained on violations of user privacy.
4.8	Devices	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Applications	See [i.2]	●	●	●	Y	Unnecessary services can be a vector for unauthorized access and should be disabled. Unnecessary services can act as spyware and collect user information.

Control 4: Secure Configuration of Enterprise Assets and Software					Imple-mentation Groups			Applicability	
Safeguard	Asset Type	Security Function	Control Title	Control Descriptions	IG1	IG2	IG3	Included?	Applicability Justification & Privacy Considerations
4.9	Devices	Protect	Configure Trusted DNS Servers on Enterprise Assets	See [i.2]		●	●	N	Using an untrusted DNS server could trick users into providing sensitive information to malicious parties, but there is no specific privacy impact.
4.10	Devices	Respond	Enforce Automatic Device Lockout on Portable End-User Devices	See [i.2]		●	●	N	This helps prevent naive attempts to access unauthorized private data. 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	See [i.2]		●	●	Y	This Safeguard can help remove personal data if a device is lost.
4.12	Devices	Protect	Separate Enterprise Workspaces on Mobile End-User Devices	See [i.2]			●	Y	Separate workspaces help enterprises easily access, manage, and delete only enterprise information. They can also assist with private usage of a mobile device.

5.5 Control 5: Account Management

The processes and tools used 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 organization, they often release passwords and other credentials to the public. Other account information can also be included within any leaked databases leak, which can include usernames and/or email addresses. Service provider accounts can also be affected.

Data Collection

Usernames, identifiers (e.g. email addresses), and credentials such as passwords 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 take biometric samples, such as iris, facial, or fingerprint scans, which are then used to create biometric templates. These templates contain uniquely personal information. It is generally unknown to an end user how this information is stored, and whether it will be kept secure.

Data Storage

Secure storage of enterprise account information and other data pertaining to authentication can be solved by implementation of several 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 are 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.

Fair Information Practice Principles:

- **The Collection Limitation Principle.** When creating an account, IT should refrain from obtaining more information than is needed.
- **The Data Quality Principle.** Any collected data should be used only for access to enterprise systems.
- **The Purpose Specification Principle.** Employees and other data subjects should be informed why their personal information is being collected and how it will be used.
- **The Use Limitation Principle.** Employees and other data subjects should be informed if this information will be used to create accounts on future systems owned by third party service providers.
- **The Security Safeguards Principle.** Care should be taken to carefully secure any stored network 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 can contain their personal data.

- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand.

- **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 and other data subjects should have the opportunity to make an informed decision on the type of personal data that will be kept as a result of account creation and maintenance. A lawful basis is needed for collecting personal data, in this case, potentially name, address, email, telephone, and other information.

- **Purpose limitation.** Users, including employees and customers, should be informed in writing about the 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 can conflict with the need to integrate the domain controller with third party software and platform. Employees and other data subjects 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.

- **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. 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 & Confidentiality**. The 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: Secure Configuration of Enterprise Assets and Software					Imple-mentation Groups			Applicability	
Safeguard	**Asset Type**	**Security Function**	**Control Title**	**Control Descriptions**	**IG1**	**IG2**	**IG3**	**Included?**	**Applicability Justification & Privacy Considerations**
5.1	Users	Identify	Establish and Maintain an Inventory of Accounts	See [i.2]	●	●	●	Y	Account inventories are likely to contain personal information, which can include PII and private data. This information needs to be appropriately protected.
5.2	Users	Protect	Use Unique Passwords	See [i.2]	●	●	●	Y	Users should be instructed to refrain from using personal information within passwords.
5.3	Users	Respond	Disable Dormant Accounts	See [i.2]	●	●	●	N	Preventing dormant accounts from being used does not have a direct impact on privacy.
5.4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	See [i.2]	●	●	●	Y	Although this is a best practice in and of itself, it can help administrators retain privacy since administrator accounts are often high value targets for malicious actors. Restricting privileges also restricts administrative managing PII and other information unless needed.
5.5	Users	Identify	Establish and Maintain an Inventory of Service Accounts	See [i.2]		●	●	Y	Depending on how service account inventories are developed, they can contain PII and private data. This information needs to be appropriately protected.
5.6	Users	Protect	Centralize Account Management	See [i.2]		●	●	Y	Centralized account management can significantly benefit an enterprise from a security perspective, but the external enterprise providing federation services can have access to personal information.

5.6 Control 6: Access Management Control

The processes and tools used 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 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 can 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 private data.

Data Collection

The information systems that help administrators manage rights and privileges within their enterprise may have collected personal information when enrolling users. Administrators and third-party service providers will generally have access to this information. 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 should 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 need to 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 data should be used only for access to enterprise systems.

- **The Purpose Specification Principle.** Employees and other data subjects should be informed why their personal information and privileges are being collected and how they will be used.

- **The Use Limitation Principle.** Employees and other data subjects should be informed if this information will be used to create accounts on future systems owned by third party service providers.

- **The Security Safeguards Principle.** Care should be taken to carefully secure any stored network 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 can contain their personal data.

- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees and other data subjects 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 and other data subjects should have the opportunity to make an informed decision on the type of personal data that will be kept 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 can conflict with the need to integrate the domain controller with third party software and platform. Employees and other data subjects 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 indefinitely for incident response and auditing purposes.

- **Integrity & Confidentiality.** The Controls can be leveraged to enable this Principle, such as Control 3: Data Protection. Employee and customer account data, including lists of access and privileges, should be protected from unauthorized access, modification, and disclosure.

Control 6: Access Management Control					Imple-mentation Groups			Applicability	
Safeguard	**Asset Type**	**Security Function**	**Control Title**	**Control Descriptions**	**IG1**	**IG2**	**IG3**	**Included?**	**Applicability Justification & Privacy Considerations**
6.1	Users	Protect	Establish an Access Granting Process	See [i.2]	●	●	●	Y	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.
6.2	Users	Protect	Establish an Access Revoking Process	See [i.2]	●	●	●	Y	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	See [i.2]	●	●	●	Y	Some remote access and multifactor authentication mechanisms log the geolocation of users when they connect.
6.4	Users	Protect	Require MFA for Remote Network Access	See [i.2]	●	●	●	Y	Some remote access and multifactor authentication mechanisms log the geolocation of users when they connect.
6.5	Users	Protect	Require MFA for Administrative Access	See [i.2]	●	●	●	Y	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.
6.6	Users	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems	See [i.2]		●	●	Y	PII and other sensitive information 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	See [i.2]		●	●	Y	Centralized access control can significantly benefit an enterprise from a security perspective, but any external organization providing these services can have access to personal information.
6.8	Data	Protect	Define and Maintain Role-Based Access Control	See [i.2]			●	N	There are no privacy impacts when using role-based access control, unless individual users are highlighted as roles within these systems.

5.7 Control 7: Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers.

Privacy Applicability

This Control focuses on using software to monitor the vulnerabilities contained within software used by an enterprise. Applying the guidance from the 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 can 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 can be problematic. Privacy implications generally do not 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 this information without the consent of the individual or required in the jurisdiction.

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 can be regulatory requirements or third-party agreements for identifying and managing vulnerabilities to systems that store privacy information. Some of these regulatory requirements can specifically call out the need for managing vulnerabilities in order to protect private information 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, 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 and other data subjects 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 and other data subjects 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 carefully secure any stored network 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 can contain their personal data.

- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees and other data subjects 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 and other data subjects should have the opportunity to make an informed decision 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 the 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. Organization 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.

- **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 & Confidentiality.** The 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: Continuous Vulnerability Management					Imple-mentation Groups			Applicability	
Safeguard	**Asset Type**	**Security Function**	**Control Title**	**Control Descriptions**	**IG1**	**IG2**	**IG3**	**Included?**	**Applicability Justification & Privacy Considerations**
7.1	Applications	Protect	Establish and Maintain a Vulnerability Management Process	See [i.2]	●	●	●	Y	Personal information about assets and specific individuals assigned to them should not be provided to vulnerability management systems.
7.2	Applications	Respond	Establish and Maintain a Remediation Process	See [i.2]	●	●	●	Y	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	See [i.2]	●	●	●	N	Using automated patch management should not have an impact on privacy.
7.4	Applications	Protect	Perform Automated Application Patch Management	See [i.2]	●	●	●	N	Using automated patch management should not have an impact on privacy.
7.5	Applications	Identify	Perform Automated Vulnerability Scans of Internal Enterprise Assets	See [i.2]		●	●	Y	Assets on an internal network can have hostnames that expose information about an individual.
7.6	Applications	Identify	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	See [i.2]		●	●	Y	Assets on an external network can have hostnames and often identifying features that can expose information about an individual.
7.7	Applications	Respond	Remediate Detected Vulnerabilities	See [i.2]		●	●	N	No privacy implications exist with remediating vulnerabilities for company owned property.

5.8 Control 8: Audit Log Management

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 can contain PII or private data.

Privacy Implications

- Logs can 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. Understanding what systems, software, libraries, and even network devices have their logs collected, and should be regularly analysed.

Data Collection

Audit logs should only be collected by third parties if explicitly agreed upon. 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. 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 privacy 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 private 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 private 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 and other data subjects should be informed what information can be stored in log files, and how the information will be used.

- **The Use Limitation Principle**. Employees and other data subjects 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 (SEIM) that is not hosted on premises.

- **The Security Safeguards Principle**. Care should be taken to carefully secure any stored log data, which likely includes PII and other personal data.

- **The Openness Principle**. Employees and other data subjects with PII and other personal data collected by enterprise systems should understand what external systems can contain their personal data.

- **The Individual Participation Principle**. This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees and other data subjects 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 and other data subjects 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 organization. A lawful basis is needed for collecting logs containing personal data.

- **Purpose limitation**. Employees and other data subjects should be informed what information can 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. Organization owned devices may not be subject to this principle.

- **Data minimization.** Nothing more than is necessary should be written to log files and then subsequently collected 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 indefinitely for incident response, auditing, and troubleshooting purposes.

- **Integrity & Confidentiality.** The 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: Audit Log Management					Imple-mentation Groups			Applicability	
Safeguard	Asset Type	Security Function	Control Title	Control Descriptions	IG1	IG2	IG3	Included?	Applicability Justification & Privacy Considerations
8.1	Network	Protect	Establish and Maintain an Audit Log Management Process	See [i.2]	●	●	●	Y	Privacy should be a major consideration in the development of an audit log management process.
8.2	Network	Detect	Collect Audit Logs	See [i.2]	●	●	●	Y	Personal devices should not have their logs collected and viewable by the enterprise unless previously discussed
8.3	Network	Protect	Ensure Adequate Audit Log Storage	See [i.2]	●	●	●	N	The size and location of audit log storage does not carry privacy considerations.
8.4	Network	Protect	Standardize Time Synchronization	See [i.2]		●	●	N	No privacy implications exist for cross-organizational time synchronization.
8.5	Network	Detect	Collect Detailed Audit Logs	See [i.2]		●	●	Y	Detailed audit logs can contain PII and other personal data. Whether this information should be collected in the first place should be considered.
8.6	Network	Detect	Collect DNS Query Audit Logs	See [i.2]		●	●	Y	DNS query logs can easily be used to track users, even on authorized personal devices accessing the network.
8.7	Network	Detect	Collect URL Request Audit Logs	See [i.2]		●	●	Y	Uniform Resource Locator (URL) request logs can easily be used to track users, even on authorized personal devices accessing the network.
8.8	Devices	Detect	Collect Command-Line Audit Logs	See [i.2]		●	●	Y	Command-line audit logs can be used to track how a user uses a system in a very granular manner.
8.9	Network	Detect	Centralize Audit Logs	See [i.2]		●	●	Y	The confluence of all audit logs can offer a very granular view into the activities of specific individuals and potentially their personal activities.
8.10	Network	Protect	Retain Audit Logs	See [i.2]		●	●	Y	Logs should only be actively stored online for specific lengths of time. Longer periods of time can exacerbate a data breach.

Control 8: Audit Log Management					Imple-mentation Groups			Applicability	
Safeguard	Asset Type	Security Function	Control Title	Control Descriptions	IG1	IG2	IG3	Included?	Applicability Justification & Privacy Considerations
8.11	Network	Detect	Conduct Audit Log Reviews	See [i.2]		●	●	Y	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.
8.12	Data	Detect	Collect Service Provider Logs	See [i.2]			●	Y	Authorized service providers collecting logs can collect PII and other personal data about employees.

5.9 Control 9: Email and Web Browser Protections

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

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 private 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 web pages.
- 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 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 can 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 maybe another repository of emails. DNS filtering offers benefits, but who is doing the filtering can have privacy implications. They can stop others from tracking a person but also allows 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.

Data Collection

Web browsers have local histories of all sites visited by the user. Browser extensions are known to collect data from users without their knowledge. Systems performing URL filtering and DNS functions will know the websites that specific users and clients visit on the network.

Data Storage

User browser history will be stored on the originating computer. This information can also be federated across all systems logged into the browser with that username and password via modern history and bookmark syncing. Some browsers offer profiles, containers and other partitioning 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.

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 can 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 can 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 employees. These extensions should be vetted by IT, cybersecurity and privacy business units within an enterprise, Browser extensions can also granularly track users, view previous browser history, read cookies, and inject content into web pages [i.12]. Some browser extensions can also contain malware. It is generally best to assume that a browser is accessing data the user is not intending and refrain from using 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 private data from employees as possible. Local regulations can require certain data to be recorded.

- **The Data Quality Principle.** Data from browsers and email systems should only be used in business. Serving ads to users based on text within an email could violate this Principle.

- **The Purpose Specification Principle.** Employees and other data subjects should be informed what information can be stored by browsers and email, and how the information will be used.

- **The Use Limitation Principle.** Employees and other data subjects 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.

- **The Security Safeguards Principle.** Care should be taken to carefully secure any browser and email data, which likely includes PII and other personal data.

- **The Openness Principle.** Employees and other data subjects with PII and other personal data collected by enterprise systems should understand what external systems can contain their personal data.

- **The Individual Participation Principle.** Employees and other data subjects 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 and other data subjects 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 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 should be configured to collect as little PII and private data from employees as possible. In addition to GDPR requirements, other local regulations can 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 and maintained for 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 can be quite useful in incident response scenarios, and therefore kept for a significant amount of time. Obsolete data should be deleted without delay.

- **Integrity & Confidentiality.** The 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 can be included there.

Control 9: Email and Web Browser Protections					Imple-mentation Groups			Applicability	
Safeguard	**Asset Type**	**Security Function**	**Control Title**	**Control Descriptions**	**IG1**	**IG2**	**IG3**	**Included?**	**Applicability Justification & Privacy Considerations**
9.1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	See [i.2]	●	●	●	N	Browsers and email clients that are unsupported should not be used. This is not included because this enhances security with no specific privacy impact.
9.2	Network	Protect	Use DNS Filtering Services	See [i.2]	●	●	●	Y	DNS filtering can help prevent tracking, but also gives the filter complete knowledge of the sites a user visits.
9.3	Network	Protect	Maintain and Enforce Network-Based URL Filters	See [i.2]		●	●	Y	This practice can help prevent an enterprise asset from downloading malware which can result in a privacy exposure. Yet this network filter will have deep knowledge on how users are accessing the enterprise network.
9.4	Applications	Protect	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	See [i.2]		●	●	Y	Browser extensions are well known for accessing and sharing information that users did not intend.
9.5	Network	Protect	Implement DMARC	See [i.2]		●	●	N	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	See [i.2]		●	●	N	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	See [i.2]			●	Y	Scanning emails can prevent phishing emails and other malicious attachments from reaching users, but this system will also be able to access private information about a user.

5.10 Control 10: Malware Defenses

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 can collect PII and other personal data (e.g. contacts, browser history).

Privacy Implications

- Spyware and adware can track what a user is doing on an infected computer. Other types of malware can 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 but 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 can also be sent outside of the network. Defensive malware tools can 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 can 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.

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 can 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 can accidentally download spyware/malware in lieu of anti-malware software.

Fair Information Practice Principles

- **The Collection Limitation Principle.** Antimalware and perimeter defense systems should be configured to collect as little PII and private data from employees as possible.
- **The Data Quality Principle.** Data from Antimalware and perimeter defense systems should only be used in security processes for defending against malware.
- **The Purpose Specification Principle.** Employees and other data subjects should be informed about the information that can be stored by Antimalware and perimeter defense systems, as well as how the information will be used.
- **The Use Limitation Principle.** Employees and other data subjects should be informed if antimalware and perimeter defense data will be transferred to other systems owned by third party service providers, such as a marketing company.
- **The Security Safeguards Principle.** Care should be taken to carefully secure any antimalware and perimeter defense data, which likely includes PII and other personal data.

- **The Openness Principle.** Employees and other data subjects with PII and other personal data collected by enterprise systems should understand what external systems can contain their personal data.

- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees and other data subjects 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 and other data subjects 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 the purpose for collecting personal data in the antimalware platform from the outset of collecting it. Personal data collected through the antimalware 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 antimalware platform is likely incidental, or a personal file can 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 antimalware system. Obsolete data should be deleted without delay.

Integrity & Confidentiality

The 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: Malware Defenses					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Control Title	Control Descriptions	IG1	IG2	IG3	Included?	Applicability Justification & Privacy Considerations
10.1	Devices	Protect	Deploy and Maintain Anti-Malware Software	See [i.2]	●	●	●	Y	Research should be done to understand the information anti-malware software can access on a system.
10.2	Devices	Protect	Configure Automatic Anti-Malware Signature Updates	See [i.2]	●	●	●	Y	Administrators for this software will likely have access to sensitive information.
10.3	Devices	Protect	Disable Autorun and Autoplay for Removable Media	See [i.2]	●	●	●	N	There are no direct privacy impacts with disabling autorun.
10.4	Devices	Detect	Configure Automatic Anti-Malware Scanning of Removable Media	See [i.2]		●	●	Y	The anti-malware software can scan personal files and collect information from these files. This information can subsequently be provided to an administrator for review.
10.5	Devices	Protect	Enable Anti-Exploitation Features	See [i.2]		●	●	N	Although these features can 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	See [i.2]		●	●	Y	Administrators for this software will likely have access to PII and private data.
10.7	Devices	Detect	Use Behavior-Based Anti-Malware Software	See [i.2]		●	●	N	Certain benign user behaviors can trigger an administrator to personally review logs.

5.11 Control 11: Data Recovery

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) records will need to be backed up, yet PII and other personal data can 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. It is 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 can 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 can 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 private information need to be stipulated in the Service Level Agreement (SLA).

Data Storage

IT can store backups offsite at an enterprise owned location. For instance, another office building that is geographically separated from the primary office. Third-party organizations providing storage for company backups can store the information in a cloud platform or at a physical hot- or cold-site. Private information 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 is 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 data.

- **The Data Quality Principle.** Data from backups should only be used during data recovery or testing.

- **The Purpose Specification Principle.** Employees and other data subjects should be informed what information can be backed up and how the information will be used.

- **The Use Limitation Principle.** Employees and other data subjects should be informed if backups will be transferred to other systems owned by third party service providers, such as a company focusing on data recovery.

- **The Security Safeguards Principle.** Care should be taken to carefully secure any backups which likely includes PII and other personal data. This includes encrypting the backups and ensuring adequate access control mechanisms are in place.

- **The Openness Principle.** Employees and other data subjects with PII and other personal data collected by enterprise systems should understand what external systems can contain their personal data.

- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees and other data subjects 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 and other data subjects 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 the purpose for collecting personal data during a backup. Personal data collected during this process can be transferred to other vendors to assist in disaster recovery or long-term data storage. Employees and other data subjects should be made aware of this.

- **Data minimization.** Nothing more than is necessary for restoration of enterprise services should be collected, but there can 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 be regularly 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 & Confidentiality.** The 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: Data Recovery					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Control Title	Control Descriptions	IG1	IG2	IG3	Included?	Applicability Justification & Privacy Considerations
11.1	Data	Recover	Establish and Maintain a Data Recovery Process	See [i.2]	●	●	●	Y	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	See [i.2]	●	●	●	Y	Automated backups should not store PII and other personal data in a form that third parties can access without the consent of the data controller or required in the jurisdiction.
11.3	Data	Protect	Protect Recovery Data	See [i.2]	●	●	●	Y	Any PII and other personal data that is backed up should be protected in the same fashion as enterprise data.
11.4	Data	Recover	Establish and Maintain an Isolated Instance of Recovery Data	See [i.2]	●	●	●	Y	There are no privacy implications of having an offsite backup of enterprise data.
11.5	Data	Recover	Test Data Recovery	See [i.2]		●	●	Y	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.

5.12 Control 12: Network Infrastructure

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 setup, 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 can 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 is best practice to regularly audit and verify who has access to private data.

Data Collection

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

Data Storage

In general, network infrastructure should not store PII and private 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, IDS, and firewalls. Since web history can be considered privacy-relevant data, 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 (including 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 privacy 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 privacy 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 and other data subjects should be informed what information will be collected by network devices and how the information will be used.
- **The Use Limitation Principle.** Employees and other data subjects should be informed if data collected by network devices will be transferred to other systems owned 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 carefully secure any network data which likely includes PII and other personal data.
- **The Openness Principle.** Employees and other data subjects with PII and other personal data collected by enterprise systems should understand what external systems can contain their personal data.
- **The Individual Participation Principle.** This is unlikely to be implemented without serious discussion with any service providers beforehand. Employees and other data subjects 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 and other data subjects 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 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 & Confidentiality.** The 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: Network Infrastructure Management					Imple-mentation Groups			Applicability	
Safeguard	Asset Type	Security Function	Control Title	Control Descriptions	IG1	IG2	IG3	Included?	Applicability Justification & Privacy Considerations
12.1	Network	Protect	Ensure Network Infrastructure is Up-to-Date	See [i.2]	●	●	●	N	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	See [i.2]		●	●	Y	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	See [i.2]		●	●	N	Systems containing private information 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)	See [i.2]		●	●	Y	Privacy protections and considerations designed into the network should be explicitly documented.
12.5	Network	Protect	Centralize Network Authentication, Authorization, and Auditing (AAA)	See [i.2]		●	●	Y	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	See [i.2]		●	●	N	This Safeguard should be applied to protect all information throughout a network, but there is no specific privacy impact.
12.7	Devices	Protect	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	See [i.2]		●	●	Y	Information systems associated with remote login or VPN capabilities will likely learn information about a user's current location.
12.8	Devices	Protect	Establish and Maintain Dedicated Computing Resources For All Administrative Work	See [i.2]			●	Y	Administrators are encouraged to use separate devices for administrative tasks and day-to-day work related tasks.

5.13 Control 13: Network Monitoring Defense

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

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, Network Monitoring 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 private information 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 can collect information about their customers.

Data Collection

Network traffic information collected by IDS, IPS, and application filtering software, alongside alerts generated from a variety of sources, can be collected.

Data Storage

Network traffic information collected by IDS, IPS, and application filtering software, alongside alerts generated from a variety of sources, are all stored. The owners of the software for all of these systems likely have access to all of this information and can store this information within their own private network. The organization 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 all PII or privacy related 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 private 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 and other data subjects should be informed what information will be collected by network devices and how the information will be used.

- **The Use Limitation Principle.** Employees and other data subjects should be informed if data collected by network devices will be transferred to other systems owned by third party service providers, such as a company focusing on forensics or incident response

- **The Security Safeguards Principle.** Care should be taken to carefully secure any network data which likely includes PII and other personal data.

- **The Openness Principle.** Employees and other data subjects with PII and other personal data collected by enterprise systems should understand what external systems can contain their personal data.

- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees and other data subjects 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 and other data subjects 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 & Confidentiality.** The 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: Network Monitoring and Defense					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Control Title	Control Descriptions	IG1	IG2	IG3	Included?	Applicability Justification & Privacy Considerations
13.1	Network	Detect	Centralize Security Event Alerting	See [i.2]		●	●	Y	Administrators should work with the enterprise Privacy Officer, or legal department, to understand what potential PII is stored in logs and alerts.
13.2	Devices	Detect	Deploy a Host-Based Intrusion Detection Solution	See [i.2]		●	●	Y	Research should be done to understand the information host-based IDS can access on a system.
13.3	Network	Detect	Deploy a Network Intrusion Detection Solution	See [i.2]		●	●	Y	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	See [i.2]		●	●	Y	Traffic filtering should in theory increase privacy for individual users and systems.
13.5	Devices	Protect	Manage Access Control for Remote Assets	See [i.2]		●	●	N	Although this Safeguard can help prevent a breach, there are no direct privacy impacts.
13.6	Network	Detect	Collect Network Traffic Flow Logs	See [i.2]		●	●	Y	Flow logs will contain detailed information about resources accessed by specific IP addresses, some of which can be statically assigned, alongside protocols used to access those resources.
13.7	Devices	Protect	Deploy a Host-Based Intrusion Prevention Solution	See [i.2]			●	Y	Research should be done to understand the information host-based IPS can access on a system.
13.8	Network	Protect	Deploy a Network Intrusion Prevention Solution	See [i.2]			●	Y	Research should be performed to understand how the IPS solution stores and collects information about individual users.
13.9	Devices	Protect	Deploy Port-Level Access Control	See [i.2].			●	N	There are no privacy impacts of using port-level access control for network access.
13.10	Network	Protect	Perform Application Layer Filtering	See [i.2]			●	Y	While these tools can help enable privacy by preventing a breach, they can store detailed information about individual users. Where that data is stored is also a concern.

Control 13: Network Monitoring and Defense					Imple-mentation Groups			Applicability	
Safeguard	Asset Type	Security Function	Control Title	Control Descriptions	IG1	IG2	IG3	Included?	Applicability Justification & Privacy Considerations
13.11	Network	Detect	Tune Security Event Alerting Thresholds	See [i.2]			●	Y	If alerts are exposing or storing sensitive information, the thresholds should be appropriately tuned.

5.14 Control 14: Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

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 the present document, 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 can make poor privacy decisions if they are not trained on appropriate use of their access and consequences of privacy breaches. 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 can 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, other than which individuals have completed privacy training.

Data Storage

The list of which employees completed privacy training is likely not the highest priority for securing. Yet this list 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. How that data is used, and protected, could be unique as there can 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 private information. The following are also relevant topics that can be included:

- understanding what data can be labeled sensitive under any applicable regulatory frameworks and compliance requirements;
- addressing private data on mobile devices, including BYOD;
- preventing, reporting, and mitigating a breach of private data;
- precautions for handling different types of privacy data;
- the risks of de-identified data being re-identified;

- use of de-identified aggregated data rather than individual data to achieve the same purpose; and
- 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. Resources for privacy training are available that include an understanding of applicable privacy law. Additionally, information is also available on promoting privacy awareness, and measuring the success of training activities.

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 do not specifically apply to cybersecurity training and awareness, but employees should be made aware of any responsibilities they have under GDPR. This can 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 & Confidentiality. N/A

Control 14: Security Awareness and Skills Training					Implementation Groups			Applicability	
Safeguard	**Asset Type**	**Security Function**	**Control Title**	**Control Descriptions**	**IG1**	**IG2**	**IG3**	**Included?**	**Applicability Justification & Privacy Considerations**
14.1		Protect	Establish and Maintain a Security Awareness Program	See [i.2]	●	●	●	Y	Establishing 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	See [i.2]	●	●	●	Y	Employees should understand when someone is attempting to obtain PII and other personal data from individuals.
14.3		Protect	Train Workforce Members on Authentication Best Practices	See [i.2]	●	●	●	Y	Some methods of authentication are more privacy preserving than others
14.4		Protect	Train Workforce on Data Handling Best Practices	See [i.2]	●	●	●	Y	Employees with responsibilities pertaining to PII and other personal data should receive specific training for how to handle this data.
14.5		Protect	Train Workforce Members on Causes of Unintentional Data Exposure	See [i.2]	●	●	●	Y	Employees with responsibilities pertaining to PII and other personal data should receive specific training for how to recognize unintentional data exposure.
14.6		Protect	Train Workforce Members on Recognizing and Reporting Security Incidents	See [i.2]	●	●	●	Y	Employees need to receive specific training about recognizing security incidents related to PII.
14.7		Protect	Train Workforce on How to Identify and Report if their Enterprise Assets are Missing Security Updates	See [i.2]	●	●	●	N	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	See [i.2]	●	●	●	Y	Employees should understand the dangers of sending private information without the appropriate security controls protecting that data.
14.9		Protect	Conduct Role-Specific Security Awareness and Skills Training	See [i.2]		●	●	Y	Employees with responsibilities pertaining to PII and other personal data should receive specific training for how to handle their private data.

5.15 Control 15: Service Provider Management

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

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, choosing providers that have privacy certifications or some other independent auditing of their own privacy practices should be considered.

Privacy Implications

- Service providers can utilize, sell, or share PII and other personal data obtained via their customers.
- Private information 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 private information has a responsibility to keep this information from being disclosed. Examples of sensitive information that can 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; and
    - 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 can collect should be clearly stated in SLAs. Specific types of data should be discussed, as should be whether the service provider can use the 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 can 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 of a service provider likely dictates the privacy rules they adhere to. Choosing a service provider from a jurisdiction without privacy or data protection laws should be considered, unless it can demonstrate adherence to high data protection standards through external certification or other trusted mechanisms.

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 should only be used while providing the product or service they were contracted for.

- **The Purpose Specification Principle.** Employees and other data subjects should be informed what information will be collected by service providers and how the information will be used.
- **The Use Limitation Principle.** Employees and other data subjects 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 carefully secure any shared data.
- **The Openness Principle.** Employees and other data subjects with PII and other personal data collected by enterprise systems should understand what external systems can contain their personal data.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand.
- **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 and other data subjects 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 their behalf and processing data from specific individuals.
- **Purpose limitation.** Employees and other data subjects 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 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 should 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 & Confidentiality.** The 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: Service Provider Management					Imple-mentation Groups			Applicability	
Safeguard	Asset Type	Security Function	Control Title	Control Descriptions	IG1	IG2	IG3	Included?	Applicability Justification & Privacy Considerations
15.1		Identify	Establish and Maintain an Inventory of Service Providers	See [i.2]	●	●	●	Y	An inventory of which service providers store what types of PII and private data should be developed and maintained.
15.2		Identify	Establish and Maintain a Service Provider Management Policy	See [i.2]		●	●	Y	Privacy expectations should be built into this service provider management policy.
15.3		Identify	Classify Service Providers	See [i.2]		●	●	Y	Providers can be classified based on access to PII, private data, and any regulations that would be applicable specifically due to private data.
15.4		Protect	Ensure Service Provider Contracts Include Security Requirements	See [i.2]		●	●	Y	For this safeguard, it is recommended that privacy requirements also be included within service provider contracts.
15.5		Identify	Assess Service Providers	See [i.2]			●	Y	Service providers should assess service providers and their defensive mitigations used to protect PII and other personal data.
15.6	Data	Detect	Monitor Service Providers	See [i.2]			●	Y	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	See [i.2]			●	Y	Once a service provider is no longer being actively used, PII and other personal data should be securely deleted from their systems.

5.16 Control 16: Application Software Security

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

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.
- Third party software libraries, components, and application programming interfaces (APIs) can collect information that they process.
- 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 appropriate security controls to third-party software developers with access to PII and other personal data.

Data Collection

Information collected by third-party software libraries and Application Programming Interfaces (APIs) can 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. Regular auditing of regulatory and 3rd party agreement requirements should be implemented to verify who has access to privacy data.

Data Storage

Security controls relating to the security of the 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. Controls and monitoring should be applied 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 private 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 towards the top end of the remediation queue.

Third-party components are a necessary commodity in modern software engineering and design. Whilst these components are often necessary, third party components handling PII should be given extra attention, inventoried, and validated accordingly. 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 a public 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 can attempt to steal private data. These modeling activities should explicitly take into account private data, with focused reviews for private datastores and other applications that access PII.

Many enterprises have privacy policies on their web sites, and customer facing applications. These policies define what information is collected, how it is used and shared, and how it is protected. Enterprises should 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 and other data subjects 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 and other data subjects 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 carefully secure any data that likely includes PII and other personal data.
- **The Openness Principle.** Employees and other data subjects with PII and other personal data collected by enterprise systems should understand what external systems can contain their personal data.
- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand.
- **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 and other data subjects 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 for 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 & Confidentiality.** The 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: Application Software Security					Implementation Groups			Applicability	
Safeguard	Asset Type	Security Function	Control Title	Control Descriptions	IG1	IG2	IG3	Included?	Applicability Justification & Privacy Considerations
16.1	Applications	Protect	Establish and Maintain a Secure Application Development Process	See [i.2]		●	●	Y	Software engineers should be trained on handling PII and other personal data.
16.2	Applications	Protect	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	See [i.2]		●	●	Y	IT systems handling PII and other personal data may need to have their vulnerabilities prioritized over others.
16.3	Applications	Protect	Perform Root Cause Analysis on Security Vulnerabilities	See [i.2]		●	●	N	Although an important activity, there is no direct privacy impact.
16.4	Applications	Protect	Establish and Manage an Inventory of Third-Party Software Components	See [i.2]		●	●	Y	Any third-party component handling PII should be afforded additional scrutiny, inventoried, and validated accordingly.
16.5	Applications	Protect	Use Up-to-Date and Trusted Third-Party Software Components	See [i.2]		●	●	N	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	See [i.2]		●	●	Y	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	See [i.2]		●	●	N	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	See [i.2]		●	●	N	Although an important Safeguard, there are no privacy specific impacts.
16.9	Applications	Protect	Train Developers in Application Security Concepts and Secure Coding	See [i.2]		●	●	N	This should happen for all developers. No privacy impact.
16.10	Applications	Protect	Apply Secure Design Principles in Application Architectures	See [i.2]		●	●	N	Secure application design principles should be applied regardless if PII data is hosted.
16.11	Applications	Protect	Leverage Vetted Modules or Services for Application Security Components	See [i.2]		●	●	N	Vetted modules and services should be leveraged regardless of datatype. There is no privacy impact.

Control 16: Application Software Security					Imple-mentation Groups			Applicability	
Safeguard	**Asset Type**	**Security Function**	**Control Title**	**Control Descriptions**	**IG1**	**IG2**	**IG3**	**Included?**	**Applicability Justification & Privacy Considerations**
16.12	Applications	Protect	Implement Code-Level Security Checks	See [i.2]			●	N	There are no privacy impacts within Code-level security checks.
16.13	Applications	Protect	Conduct Application Penetration Testing	See [i.2]			●	Y	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	See [i.2]			●	Y	Threat modeling activities should include additional and focused review for private datastores and other applications that access that data.

5.17 Control 17: Incident Response and Management

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

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 private 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 can have access to private information. 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 private information. They can intentionally abuse or improperly handle their access to this information

- Cyber incidents often have a privacy component due to what enterprises resources were accessed, or what data was exfiltrated. This often brings local and federal and national privacy law into account. These laws can have specific mechanisms and timeframes for notifying the government and affected entities of a cybersecurity incident or data breach. Organizations that do not appropriately notify can face fines or other legal action.

- Data breaches affecting PII need to be reported to the appropriate entities within prespecified 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 can also obtain access to this data. It may be prudent to redact certain portions of information and obtain a non-disclosure agreement before providing this information to other entities.

Data Storage

All data collected during incident response activities need to be protected as it is often private information but also can be needed for upcoming legal proceedings. Collected information can be stored outside of the primary enterprise, within a third-party incident response organization's management platform. It is important to protect forensic data, and the 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 can 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 and other data subjects 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 and other data subjects 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 carefully secure any data that likely includes PII and other personal data.

- **The Openness Principle**. Employees and other data subjects with PII and other personal data collected by an incident response team should understand what external systems can contain their personal data.

- **The Individual Participation Principle**. This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees and other data subjects 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 and other data subjects 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, but 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 can 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 & Confidentiality.** The 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: Incident Response Management					Implementation Groups			Applicability	
Safeguard	**Asset Type**	**Security Function**	**Control Title**	**Control Descriptions**	**IG1**	**IG2**	**IG3**	**Included?**	**Applicability Justification & Privacy Considerations**
17.1		Respond	Designate Personnel to Manage Incident Handling	See [i.2]	●	●	●	Y	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	See [i.2]	●	●	●	Y	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	See [i.2]	●	●	●	Y	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	See [i.2]		●	●	Y	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	See [i.2]		●	●	Y	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.
17.6		Respond	Define Mechanisms for Communicating During Incident Response	See [i.2]		●	●	Y	Any communication methods should meet any regulatory or compliance requirements for privacy breaches.
17.7		Recover	Conduct Routine Incident Response Exercises	See [i.2]		●	●	Y	Incident response procedures dealing with privacy breaches should be regularly exercised.
17.8		Recover	Conduct Post-Incident Reviews	See [i.2]		●	●	Y	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	See [i.2]			●	Y	Security event thresholds should be established for cyber incidents that involve PII and other personal data.

5.18 Control 18: Penetration Testing

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

Privacy Applicability

This Control focuses on how to effectively simulate the actions of an external and/or internal attacker within an enterprise environment. This can 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 can 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. When penetration testing is performed by an external organization, 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 organization.

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 and other data subjects should be informed what information could be collected by penetration testers and how the information will be used.
- **The Use Limitation Principle.** Employees and other data subjects 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 carefully secure any data that likely includes PII and other personal data.

- **The Openness Principle.** Employees and other data subjects with PII and other personal data collected by penetration testers should understand what external systems can contain their personal data.

- **The Individual Participation Principle.** This is unlikely to be implementable without serious discussion with any service providers beforehand. Employees and other data subjects 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 and other data subjects 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 & Confidentiality.** The 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: Penetration Testing					Imple-mentation Groups			Applicability	
Safeguard	Asset Type	Security Function	Control Title	Control Descriptions	IG1	IG2	IG3	Included?	Applicability Justification & Privacy Considerations
18.1		Identify	Establish and Maintain a Penetration Testing Program	See [i.2]		●	●	Y	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	See [i.2]		●	●	Y	External penetration testers should be made aware of systems that contain private 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	See [i.2]		●	●	Y	Penetration testing findings in systems containing PII and other personal data should be prioritized for remediation.
18.4	Network	Protect	Validate Security Measures	See [i.2]			●	Y	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	See [i.2]			●	Y	Internal tests should abide by the rules of engagement for dealing with systems containing PII and private data.

Annex A: Bibliograpy

- FIRST: "Common Vulnerability Scoring System SIG".

NOTE: Available at https://www.first.org/cvss/.

- IEEE: "DDoS in the IoT: Mirai and Other Botnets".

NOTE: Available at https://ieeexplore.ieee.org/abstract/document/7971869.

- Cybersecurity & Infrastructure Security Agency Computer Emergency Response Team.

NOTE: Available at https://www.cisa.gov/uscert/.

- Industrial Control Systems Information Sharing and Analysis Center (ICS-ISAC).

NOTE: Available at http://ics-isac.org/blog/.

- Mobile version of MITRE ATT&CK®.

NOTE: Available at https://attack.mitre.org/tactics/mobile/.

- NIST SP 800-160 Revision 1: "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems".

NOTE: Available at https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final.

- OWASP IoT Project.

NOTE: Available at https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project.

- OWASP Web Security Testing Guides.

NOTE: Available at https://owasp.org/www-project-web-security-testing-guide/.

- IEEE™: "Towards a Definition of the Internet of Things".

NOTE: Available at https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.

- National Academies of Sciences: "Privacy Research and Best Practices: Summary of a Workshop for the Intelligence Community".

NOTE: Available at https://www.dni.gov/files/documents/CLPO/NAP%20Privacy%20Research%20and%20Best%20Practices.pdf.

- Department of Homeland Security: "Privacy Training & Awareness".

NOTE: https://www.dhs.gov/privacy-training.

- US Nuclear Regulatory Commission: "Privacy Program".

NOTE: Available at https://www.nrc.gov/privacy/index.html.

- California Department of Aging: "Privacy & Information Security Awareness Training".

NOTE: Available at https://www.aging.ca.gov/Information_Security/Privacy_and_Information_Security_Awareness_Training/.

History

Document history		
V1.1.1	September 2018	Publication
V2.1.1	February 2023	Publication