Center for Internet Security®

CIS Controls

Privacy Implications Guide

for the CIS Controls™ *(Version 6)*

(January 12, 2017)

Privacy Implications Guide for the CIS Controls (Version 6)

Acknowledgements:

CIS gratefully acknowledges the contributions provided by Maryellen Callahan, Chair of Jenner & Block's Privacy and Information Governance Practice; Rick Doten, Chief of Cyber and Information Security at the Crumpton Group; and other expert volunteers from the CIS Community for the content and editing of this guide.

Privacy Implications Guide for the CIS Controls (Version 6)

Introduction

Many professionals within the cyber security industry struggle to understand the differences between privacy and security. Some view both as an interrelated means to an end: privacy means using encryption to protect confidentiality. This confusion makes it challenging for IT professionals to protect privacy effectively: you can't have privacy without security, but can have security without privacy. Additionally, legal staff grapples with the implications of changes in technology that often outpace the law.

This document is a companion to the CIS *Controls for Effective Cyber Defense v. 6* (CIS Controls), which are a set of prioritized best practices designed to protect information systems and assets against internal and external threats. The Privacy Guide supports these objectives by aligning privacy principles and highlighting potential privacy concerns that are implicated by the CIS Controls. The CIS Controls provide guidelines and examples for IT security programs by describing a comprehensive list of key security areas to be addressed, including threats to personal information and privacy. This Guide is intended to identify opportunities to integrate privacy considerations into data security controls.

Audience and Use of Privacy Guide

The National Academy of Sciences (NAS) Privacy Research and Best Practices report poses 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."

This Privacy Guide is a resource meant for both IT Security professionals who are familiar with the CIS Controls, and privacy or legal staff within organizations. The document hopes to provide bridging information for both IT Security professionals looking to better understand how privacy applies to IT security controls and privacy or legal professionals who need to better understand how modern technology and IT processes might impact privacy.

We hope that the document starts a line of communication between these two key groups, and enhances the governance process by which business and legal management communicate with IT and IT security teams. Proper data governance will

help to better understand the privacy implications and develop and implement appropriate privacy controls. We hope that privacy professionals learn about the CIS Controls and how it can be a tool to support privacy requirements.

This Guide should be a good starting point to establish a constructive dialogue and cooperation among all groups. The Privacy Guide is useful for enterprises of any size: large organizations that might not have good communication between IT and legal teams and Small/Medium Enterprise (SMEs) that might not know what they need to know. The Guide outlines some the privacy implications of the CIS Controls and suggests mitigation approaches.

Topics like regulatory requirements, data protection standards, requirements within partner agreements, and breach disclosure laws might not be known to technical staff who should understand what they need to prepare for reporting. There is no silver bullet to approaching privacy considerations as they are often complex and will vary by country, state, industry, customer type and other factors.

Scope of this document

In noting privacy implications of the CIS Controls and suggesting mitigations, this document focuses on privacy requirements and best practices for enterprises. It takes a broad view of international privacy laws as they vary from country to country and provides guidance on what is needed for organizations to make their own risk-based decisions. As such, it is critical that IT security and privacy/legal teams work together.

While a full-scope privacy and security guide could run thousands of pages, this Guide is only meant as a starting point to outline the most essential processes that every organization should focus on when dealing with data privacy and security concerns. Although the following topics fall outside the scope of the Guide, we encourage organizations to be mindful of the following issues, where applicable:

- Evolving national and international laws
- Safe Harbor's replacement by Privacy Shield in the EU
- Breach disclosure requirements nationally, regionally, and internationally
- Big Data analysis, issues of secondary use, and derived data
- Privacy related to personal mobile devices used in the enterprise

- Privacy for Internet of Things (IoT), such as personal wearable devices, autos, smart homes, etc.

Privacy Principles

The following overarching privacy principles should be discussed between IT Security and corporate privacy or legal teams within any organization:

- Privacy is based on the Fair Information Practice Principles: Transparency, Individual Participation, Collection Limitation, Purpose Specification, Use Limitation, Data Quality, Security, and Accountability.
- Privacy is a human right in Europe. In the United States, influential scholars and jurists have defined privacy as a legal right, like "the right to be let alone," or an individual's right "to control, edit, manage, and delete information about them[selves] and decide when, how, and to what extent information is communicated to others."
- Privacy is a value; it is normative and varies among cultures in its particulars. For example, an individual's financial information is considered personal information requiring protection in the U.S., but not in Europe; an individual's business contact information (e.g., business email address or phone number) is considered personal in Europe, but not in the U.S.
- Security is not normative; it is about building systems that perform according to specifications, including specifications to implement policies on privacy.
- Privacy is not just the C of the security triad of **C**onfidentiality, **I**ntegrity, and **A**ccessibility.
- Security is essential to privacy: it is one of the foundational principles of privacy.

CIS Controls (Version 6): Privacy			
CSC #	**Control Name**	**Privacy Implications**	**Privacy Mitigation Suggestions**
1	Inventory of Authorized and Unauthorized Devices	Computing assets are usually tied to employees. Knowledge about a device and where it is located could provide a link to an individual. • There might be issues with the name of individual tied to device (if device name is also user name). • Sometimes organizations issue different devices based on role, for instance developers might get more powerful laptops than general staff; or executives might get tablets. Knowledge of this could allow enumeration of user's role. • With personal mobile devices, device management might track location of that device at any given time, which could determine whereabouts of a user.	Technical staff should work with corporate privacy officer, or legal counsel to identify what requirements are needed for privacy data protection. Device inventories should be protected as personal information. Enterprises should have a privacy policy that lets users know the privacy risks of mobile devices, and what could be derived from the devices they have.
2	Inventory of Authorized and Unauthorized Software	Applications, tied to devices, that are tied to individuals may hold personal data, or allow someone to gleam	Technical staff should work with corporate privacy officer, or legal counsel to identify what requirements are needed for privacy data protection.

CIS Controls (Version 6): Privacy			
	Control Name	**Privacy Implications**	**Privacy Mitigation Suggestions**
		information about that user. • Some software applications may contain personal information (e.g., employer-sponsored wellness applications or financial). • When managing apps on mobile devices, there might be issues with certain personal applications 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.	In the inventory, identify applications likely to contain personal or confidential information. Apply appropriate protections to the inventory and to sensitive applications. Note: A data inventory and classification process can be coordinated with the initial creation and maintenance of the software inventory. Software inventories of employee personal mobile devices should be protected as personal information. Enterprises should have a privacy policy that lets users know these characteristics, and what could be derived from the devices they have.
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	There are often regulatory requirements, or 3rd party agreements for security controls on systems that store privacy information • The security configurations could be a compliance requirement; or if there is a breach, their absence	Make sure there is a data governance process that identifies all PII or privacy related data, where it is stored, and the data flow of that data. That way, appropriate protections can be applied to all systems in the data flow chain. Implement auditing of regulatory and 3rd party agreement requirements to verify the location and appropriate protection of all privacy data.

CIS Controls (Version 6): Privacy			
	Control Name	**Privacy Implications**	**Privacy Mitigation Suggestions**
		could prove lack of sufficient controls to protect data.	
4	Continuous Vulnerability Assessment and Remediation	There might be regulatory requirements or 3rd party agreements for identifying and managing vulnerabilities to systems that store privacy information. • Similar to managing secure configurations, the identification of vulnerabilities that could allow unauthorized access to privacy data could be a compliance issue, or lead to a breach, which would require disclosure. • If there is a breach, inadequate vulnerability management could prove lack of sufficient controls to protect data.	Applying the guidance from the CIS Controls for vulnerability management will contribute to situational awareness of vulnerability and being to be proactive about potential weaknesses in privacy controls.
5	Controlled Use of Administrative Privileges	Administrators of systems, applications, and databases have full access to any data stored on the platform. • For PII or PHI data, there is no business need for sys admins to	Technical staff should work with corporate privacy officer, or legal counsel to identify what requirements are needed for privacy data protection, including the monitoring of users with administrative privileges, as legally allowed There are tools that can limit administrative access to privacy data at the system or application level. These tools also can

CIS Controls (Version 6): Privacy			
	Control Name	**Privacy Implications**	**Privacy Mitigation Suggestions**
		have access to this data. Failure to control access could be a compliance requirement, or could lead to unauthorized access and require disclosure. • Control recommends multi-factor authentication; some implementations log geolocation of the user is at time of login.	monitor access, and set alerts for unauthorized access, or provide log reports to prove administrators did not access data. Implement auditing of regulatory and 3rd party agreement requirements to verify the location and appropriate protection of all privacy data.
6	Maintenance, Monitoring & Analysis of Audit Logs	Some access or error logs from applications might contain privacy data. • There might be issues with type of data that is collected, especially about user activity, personal information within an activity log. • It is possible that privacy data is logged or cached at the system or application level.	Make sure there is a data governance process that identifies all PII or privacy related data, and where it is stored, and the data flow of that data, including what is logged Administrators should work with corporate Privacy Officer, or legal department, to understand what potential PII is stored in logs and alerts, and that data should be protected at the same level as the data itself, including appropriate retention limits.

CIS Controls (Version 6): Privacy			
	Control Name	**Privacy Implications**	**Privacy Mitigation Suggestions**
7	Email and Web Browser Protections	Email is the most prominent business communication channel, the email server holds all emails sent by users from their work accounts, be they business or personal. Most large organizations have gateways for protection and monitoring of email and web traffic, which store activity about web searches, and are another repository of emails. Web browsers have local histories of all sites visited by the user. There are tracking cookies used by web sites to "follow and record" all the sites visited by a user; additionally, web browsers sometimes have vulnerabilities that allow external sites to capture privacy data. Personal information could be within emails, history of web activity, or capture of personal information in event logs.	Administrators should work with corporate Privacy Officer, or legal department, to understand what potential PII is stored in web and email logs and alerts, and that data should be protected at the same level as the data itself. Users will need to be trained on appropriate email and web activity related to handling privacy data. They should not send privacy data over unencrypted channels, or to non-authorized locations or individuals. Similar to CSC 2, the regular updating and patching of web browsers, as well as use of script-blocking add-ons, or restrict use of applications, such as Flash, will contribute to protecting user privacy and that of others whose personal information users handle.

CIS Controls (Version 6): Privacy			
	Control Name	**Privacy Implications**	**Privacy Mitigation Suggestions**
8	Malware Defenses	Sometimes malware collects personal information, such as contacts. Sometimes the alerts or logs from endpoint or perimeter malware defenses contain this data. Malware might collect and send privacy data outside of the network over insecure channels. Some host and perimeter malware tools might record sensitive data. These alerts and logs could contain privacy information that should be protected accordingly.	Administrators should work with corporate Privacy Officer, or legal department, to understand what potential PII is stored in logs and alerts, and that data should be protected at the same level as the data itself.
9	Limitations and Control of Network Ports, Protocols and Services	There are often regulatory requirements for secure configurations and controls on systems that store privacy information • The security configurations could become a compliance requirement; or if there is a breach, they could prove lack of sufficient controls to protect data.	Make sure there is a data governance process that identifies all PII or privacy related data, where it is stored, and the data flow of that data. That way, appropriate protections can be applied to all systems in the data flow chain. Implement auditing of regulatory and 3rd party agreement requirements to verify the location and appropriate protection of all privacy data.

CIS Controls (Version 6): Privacy			
	Control Name	**Privacy Implications**	**Privacy Mitigation Suggestions**
10	Data Recovery Capability	Personal data might be backed up and stored in an insecure manner, or in a country that violates the privacy requirements regarding the data subjects.	Make sure data governance process identifies all PII and privacy related data. Develop backup plans that account for any specific privacy protections, or geographic restrictions. Implement auditing of regulatory and 3rd party agreement requirements to verify the location and appropriate protection of all privacy data.
11	Secure Configurations for Network Devices such as Firewalls, Routers and Switches	There are often regulatory requirements, or 3rd party agreements for security controls on devices that route privacy data within or between networks. • Network and security device configurations could be a compliance requirement; or if there is a breach, they could prove the lack of sufficient controls to protect data.	Make sure 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. That way, appropriate protections can be applied to all systems in the data flow chain. Implement auditing of regulatory and 3rd party agreement requirements to verify the location and appropriate protection of all privacy data.

CIS Controls (Version 6): Privacy			
	Control Name	**Privacy Implications**	**Privacy Mitigation Suggestions**
12	Boundary Defense	There might be issues with the type of data that is collected, especially about user activity, email logs, or personal information within an activity log to web sites. • The security architecture could become a compliance requirement; or if there is a breach, insufficient perimeter controls could prove lack of sufficient controls to protect data.	Make sure 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. Make sure you know what data is recorded in perimeter security tools. These alerts and logs could contain privacy information that should be protected accordingly. Implement auditing of regulatory and 3rd party agreement requirements to verify the location and appropriate protection of all privacy data.

CIS Controls (Version 6): Privacy			
	Control Name	**Privacy Implications**	**Privacy Mitigation Suggestions**
13	Data Protection	This control recommends data loss prevention tools, which can collect PII. As part of that process, sweeps of devices can reveal PII. • The security configurations could become a compliance requirement; or if there is a breach, they could prove lack of sufficient controls to protect data. • Incorrect implementation of encryption, use of weak encryption algorithms, or insecure management of encryption keys could lead to privacy risks.	Make sure there is a data governance process that identifies all PII or privacy related data, where it is stored, and the data flow of that data. That way, appropriate protections can be applied to all systems in the data flow chain. Be sure to address portable devices and media that may carry PII. Implement auditing of regulatory and 3rd party agreement requirements to verify the location and appropriate protection of all privacy data.
14	Controlled Access Based on the Need to Know	Privacy is not simply a matter of protecting data from unauthorized access, but also of the appropriate use of data by those with business need to access the data.	Make sure there is a data governance process that identifies all PII or privacy related data, where it is stored, and who should have access. Apply controls and monitoring to these accounts. Implement regular auditing of regulatory and 3rd party agreement requirements to verify who has access to privacy data.

CIS Controls (Version 6): Privacy			
	Control Name	**Privacy Implications**	**Privacy Mitigation Suggestions**
15	Wireless Access Control	Wireless access is ubiquitous. Within an organization, guests might connect their personal, or their company-issued devices, and employees might connect their personal devices to local WiFi. • Be aware of what information is collected about the device, and whether it might have privacy protection requirements, or whether certain information should not be collected on citizens of some countries, or data on WiFI networks in offices of those countries. • There might be issues with type of data that is collected, could relate to tracking of device, or user activity, personal information within an activity log.	Make sure there is a data governance process that identifies all PII or privacy related data, where it is stored, and the data flow of that data. That way, appropriate protections can be applied to all systems in the data flow chain. For example, a separate WiFi network for use by guests, prevents them from accessing the regular organizational network. Implement auditing of regulatory and 3rd party agreement requirements to verify the location and appropriate protection of all privacy data.

CIS Controls (Version 6): Privacy			
	Control Name	**Privacy Implications**	**Privacy Mitigation Suggestions**
16	Account Monitoring and Control	In the USA, employees have only limited expectations of privacy for their accounts on corporate networks. But in other countries, there are still expectations of privacy, even on company networks. For multinational companies, it's important to know these rules. • There could be information about when and where a users accesses information. • Some remote access and multifactor authentication mechanisms log the geolocation of users when they connect. • While this visibility is appropriate for tracking unusual activity, such as a user known to be in one location logging in from another. Or for investigations, to see where a user was at time of a login, there are countries where this could be a privacy issue for their citizens.	Make sure there is a data governance process that identifies all PII or privacy related data, where it is stored, and who should have access. Apply controls and monitoring to these accounts. Implement regular auditing of regulatory and 3rd party agreement requirements to verify who has access to privacy data. Be aware of the citizenship of users, and the privacy requirements for any international offices of your organizations.

CIS Controls (Version 6): Privacy			
	Control Name	**Privacy Implications**	**Privacy Mitigation Suggestions**
17	Security Skills Assessment and Appropriate Training to Fill Gaps	*This is a privacy training opportunity*	Training all levels of technical staff on privacy, socializing privacy policies to users, and promoting good behavior in protecting privacy information are opportunities to improve overall enterprise privacy programs. Coordinate or integrate privacy and security training for staff.
18	Application Software Security	Applications can be primary collectors of privacy information, and the application of this control could introduce issues if this data is logged or recorded as part of error or event log. • Generally the guidance in this control promotes privacy. • 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's important to evaluate all logs, backups, and cache stores where privacy data might be permanently or temporarily stored.	Make sure there is a data governance process that identifies all PII or privacy related data, where it is stored, and who should have access. Apply controls and monitoring to these accounts. Implement regular auditing of regulatory and 3rd party agreement requirements to verify who has access to privacy data. Most organizations must have privacy policies on their web sites, and customer facing applications (web or mobile). These policies define what information is collected, how it's used and shared, and how it's protected. Consider having and posting a privacy policy for internal business applications.

CIS Controls (Version 6): Privacy			
	Control Name	**Privacy Implications**	**Privacy Mitigation Suggestions**
19	Incident Response and Management	There could be personal information revealed or collected as part of data collection for an incident. Protection of this information is important for privacy. • There are packet capture tools that organizations use to as a source of evidence with doing investigations. Because they log all data to the web, these tools often have privacy information from employees accessing their personal financial or healthcare accounts.	Build data breach reporting requirements into incident response plans. While conducting an investigation, or collecting evidence for forensics, work with privacy or legal team to understand what data might have privacy requirements and protect that data appropriately. This includes possibly redacting it in reports that could have wide distribution. Consider legal team overseeing incidents to allow organizations to mark incident reports as “attorney client privileged.” Description of incident response of forensic procedures should be in the employee privacy statement, so employees are aware. It is important to protect forensic data, and the access to this data similar to other privacy data.

CIS Controls (Version 6): Privacy			
	Control Name	**Privacy Implications**	**Privacy Mitigation Suggestions**
20	Penetration Tests and Red Team Exercises	There could be personal information revealed or collected as part of the testing process, especially with Phishing. Protection of this information could be an issue. • In addition to the considerations in the incident response Control #19, part of modern penetration testing is social engineering. This involves collecting information about targets to use in the scam. Some methodologies send phishing emails to targets to send them to sites to enter personal information, later used for social engineering or to reset a password with help desk.	Penetration testers should be informed by privacy or legal teams on what data is considered privacy data, and to limit the collection of that data, protect any privacy data collected appropriately, an not include PII in reports. Consider legal team overseeing penetration testing to allow organizations to mark findings reports as “attorney client privileged.”

Privacy References

- National Academy of Sciences: Privacy Research and Best Practices
- The CIS Controls Privacy Impact Assessment Companion
- OASIS Privacy management reference model
- EU General Data Protection Regulation
- EU Privacy Shield
- Privacy by Design: the 7 Foundational Principles
- OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata
- Department of Homeland Security, Fair Information Practice Principles: Framework for Privacy Policy, https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf
- Organization for Economic Co-operation and Development (OECD) Privacy Principles: http://oecdprivacy.org/
- Robert Gellman, FAIR INFORMATION PRACTICES: A Basic History: http://bobgellman.com/rg-docs/rg-FIPShistory.pdf