Data Management Policy Template

**CIS Critical Security Controls**

**November 2022**

# Contents

[Contents 2](#_Toc117434230)

[Acknowledgments 3](#_Toc117434231)

[Introduction 4](#_Toc117434232)

[Purpose 4](#_Toc117434233)

[Types of Data 4](#_Toc117434234)

[Scope 4](#_Toc117434235)

[Data Lifecycle 6](#_Toc117434236)

[Data Management Policy Template 9](#_Toc117434237)

[Purpose 9](#_Toc117434238)

[Responsibility 9](#_Toc117434239)

[Exceptions 9](#_Toc117434240)

[Policy 9](#_Toc117434241)

[Revision History 12](#_Toc117434242)

[Appendix A: Acronyms and Abbreviations 13](#_Toc117434243)

[Appendix B: Glossary 14](#_Toc117434244)

[Appendix C: Implementation Groups 16](#_Toc117434245)

[Appendix D: CIS Safeguards Mapping 17](#_Toc117434246)

[Appendix E: References and Resources 18](#_Toc117434247)

# Acknowledgments

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

**Editors:**

Joshua M Franklin, CIS  
Ginger Anderson, CIS

**Contributors:**

Dave Tchozewski   
Tony Krzyzewski, SAM for Compliance Ltd  
Jon Matthies   
Edsel Medina   
Staffan Huslid, Truesec  
Jamie Fike  
Ken Muir   
Luke McFadden   
Diego Bolatti, Information Systems Engineer, Universidad Tecnológica Nacional (Argentina)   
Bryan Chou  
Bryan Ferguson  
Keala Asato  
Paul Flatt  
Gavin Willbond, SSS - IT Security Specialists  
Robin Regnier, CIS   
Valecia Stocchetti, CIS

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License. (The link can be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>.)

To further clarify the Creative Commons license related to the CIS Controls® content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization, and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to <http://www.cisecurity.org/controls/> when referring to the CIS Controls in order to ensure that users are employing the most up-to-date guidance. Commercial use of the CIS Controls is subject to the prior approval of the Center for Internet Security, Inc. (CIS®).

# Introduction

An enterprise’s traditional boundaries no longer contain the entirety of an enterprise’s data. The enterprise holds data related to finances, intellectual property, customer, and personnel data. Data is stored in the cloud, on phones and tablets, and even sensitive data is often shared with service providers located all over the world. The enterprise’s loss of control over protected or otherwise sensitive data is a serious and often reportable business impact to include running afoul of local or national data regulations for protection of personal data. Data compromise may occur as a result of theft or espionage, or merely poorly understood data management rules and user error.

## Purpose

The CIS Critical Security Controls® (CIS Controls®) recommends several policies that an enterprise should have in place as foundational elements of its cybersecurity program. This *Data Management Policy* is meant as a “jumping off point” for enterprises that need help drafting their own enterprise data management policy. Enterprises are encouraged to use this policy template in whole or in part. With that said, there are multiple decisions points and areas that must be tailored to your enterprise. In CIS Controls v8, Control 3 states:

**Control 3 – Establish and Maintain a Data Management Process**

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

To support this Safeguard, it is important for an enterprise to develop a data management process. This process should include a data management framework and requirements for handling, storing, and disposing of data. Additionally, there should also be a data breach process that integrates with the incident response plan, and other associated compliance and communication plans. This document supports the development of a process for managing and protecting data in the enterprise and the implementation of Safeguards in this CIS Control.

## Types of Data

There are many types of data that can be housed and managed by an enterprise, including, but not limited to, the following:

* Financial Data, such as payroll, tax, banking, credit card data, etc.
* Personally Identifiable Information (PII) and Human Resource data to include Social Security Numbers (SSNs), health information, home addresses, birth dates, etc.
* Trade secrets, research, patented technologies, other forms of intellectual property, etc.
* Data used to support customer facing applications
* Personal data
* Metadata (e.g., file size, file type, data of data, source)
* Information pertaining to the management of information systems (e.g., network diagrams)

## Scope

This policy template is meant to supplement the CIS Controls v8. The policy statements included within this document can be used by all CIS Implementation Groups (IGs), but are specifically geared towards Safeguards in Implementation Group 1 (IG1). In [Appendix D](#_Appendix_D:_CIS), Safeguards unique to IG1 are specifically highlighted for ease of use. For more information on the CIS Implementation Groups, see [Appendix C](#_Appendix_C:_Implementation). Additionally, a glossary in [Appendix B](#_Appendix_B:_Definitions) is provided for guidance on terminology used throughout the document. Future versions of this template may expand the scope to both Implementation Group 2 (IG2) Safeguards. IG2 and IG3 enterprises may feel the need to add sections that go beyond IG1, and are welcome to do so. Depending on an enterprise’s sector or mission, other policy statements may also need to be added or removed. This is encouraged as this policy needs to be molded and fit to the enterprise’s needs

# Data Management Lifecycle

Identifying and tracking data is an important process in the *Data Lifecycle*. In order to protect data, an enterprise must first know what data is housed within the enterprise. In addition, many other CIS Safeguards and Controls are dependent on the data inventory, such as account management, access control, and more. Shown below in Figure 2 are the high-level “steps” of the *Data Management Lifecycle*, followed by a detailed description of what each step entails.

Diagram

Description automatically generated

Figure 1. Data Management Lifecycle Diagram

* **Data Acquisition** – The process of gathering data which can then be displayed, stored, and analyzed.
* **Data Inventory** – A record of all data relevant to an enterprise for analysis, decision-making, or other justifiable need.
* **Data Classification** – Organizing data by categories that can be used to dictate protection and security efforts by priority.
* **Data Protection** – The process of safeguarding data from corruption, compromise, or loss.
* **Data Handling** – The process of ensuring that data is stored in a safe and secure manner during usage and afterward.
* **Data Disposal** – The process of removing enterprise data from enterprise assets, to include hard paper copies.

Note that these topics fall under CIS Control 3: *Data Protection*. In time, as a company matures, many of these Safeguards may require their own, separate policies to better suit their needs. A data management process may also include elements that do not directly pertain to cybersecurity such as data governance, stewardship, access, quality, publishing, and maintenance; This policy template does not contain policy statements for these elements.

**Data Acquisition**

Data acquisition is the process of creating, collecting, and organizing information. The data may be created or collected using a variety of enterprise assets and sensors. Data acquired is usually of value to the enterprise operationally or analytically. When acquiring data, an enterprise must consider storage solutions and security requirements that are commensurate with the type of data collected. Enterprises must consider access of the data to include who, how, and when data can be accessed.

**Data Inventory**

Knowledge of an enterprise’s assets, to include data, is critical to cybersecurity. The first step in this process is to understand the types of data an enterprise owns and where this data is located. A data inventory helps to solve this problem. Similar to an enterprise asset or software inventory, the data inventory focuses on assessing the types of data an enterprise generates. The individual ultimately responsible for safeguarding, maintaining, and shepherding the data, is commonly referred to as the *data owner*. Many types of information systems, such as laptops, firewalls, or sensors, will create data in the form of logs or telemetry. Many enterprises center their entire business model around the collection, analysis, manipulation, and selling of data. All types of data an enterprise leverages should be included in the data inventory.

The [Johns Hopkins University Center for Government Excellence](https://labs.centerforgov.org/data-governance/data-inventory/) defines a data inventory as *“… a fully described record of the data assets maintained by a city. The inventory records basic information about a data asset including its name, contents, update frequency, use license, owner/maintainer, privacy considerations, data source, and other relevant details. The details about a dataset are known as metadata.*” They also provide a number of plans from state and regional governments that focus on data inventory from a research and data analysis perspective. Another guide for performing data inventories includes the [U.S. National Park Service’s Data Management Guidelines for Inventory and Monitoring Networks](https://irma.nps.gov/DataStore/DownloadFile/152590).

Components of a data inventory may include:

* **Identifier** – This can be a filename or other unique identifier.
* **Data type** – Financial, PII, or other type of data.
* **Data owner** – The individual or business unit entrusted with the data.
* **Data classification/label** – While data classification is not an IG1 requirement, enterprises should, at a minimum capture data sensitivity using sensitive or non-sensitive categories. If capable, enterprises can further classify data using topic area (e.g., PII).
* **Data location** – Where the data is stored.
* **Data format** – Type of file, which may be database or long-term storage device/service.
* **Data retention** – Required time frame for retention of data for legal, regulatory, or business requirements.

**Data Classification**

Enterprises should determine what data is considered sensitive based on legal, regulatory, or business requirements as well as potential risk posed should data be compromised or lost. At a minimum, the enterprise should use one of two categories to describe the data: sensitive and non-sensitive. If possible, enterprises should further describe data using industry specific categories such as PII, financial, customer, etc. Enterprises should also consider categories such as confidential, public, commercial, proprietary/internal, and others as applicable and appropriate. Managing granular and descriptive labels can be a time intensive, on-going task, and enterprises should choose what aspects of data classification process are most pertinent to their enterprises.

**Data Protection**

Data protection is comprised of data security and data privacy. It is important to ensure data is secured via appropriate measures such as access control, encryption, threat monitoring, etc. These measures should be dictated by the sensitivity of the data and data privacy requirements such as legal, regulatory, and business requirements. Many aspects of the CIS Controls describe appropriate protections that an enterprise should implement.

**Data Handling**

Data handling entails properly securing the data throughout the whole lifecycle including the processing, storage, and transmission of the data, in accordance with data sensitivity. Lacking specific guidance to dictate the length of retention of data from production system, enterprise data can become cumbersome to manage, which may lead to accidental data loss or mismanagement. This is in part due to data being stored nowadays essentially everywhere, within the enterprise, outside the enterprise, and with third-party service providers. Additionally, removal of sensitive data no longer being used lessens the impact of a data breach since less information will be available to be stolen on enterprise assets.

Enterprises should work to understand the relevant laws regarding data retention and their enterprise, such as the General Data Protection Regulation (GDPR). This is especially so if they are housing data that is covered by special legislation, such as medical information. Certain laws may specify timeframes that enterprises must keep data safe or mandate specific methods of destruction. Examples of a data retention schedule include this document from the [National Aeronautics and Space Administration](https://nodis3.gsfc.nasa.gov/NPR_attachments/NRRS_1441.1A.pdf). Enterprises may wish to draft additional policies for retention timeframes for certain classes of data or data labels. The Colorado Department of Education provides a [sample Data Retention Policy](https://www.cde.state.co.us/dataprivacyandsecurity/sampleitpolicies) that can be helpful. A barebones template for this is provided.

*Department Name*

|  |  |  |  |
| --- | --- | --- | --- |
| File Type | Data Label | Media Format | Retention Period |
|  |  |  |  |
|  |  |  |  |

**Data Disposal**

The act of removing data from enterprise systems helps to alleviate data storage and maintenance resources (e.g., cloud or physical storage, staff time to appropriately maintain data) and help reduce the impact of a data breach. The variety of data storage mediums used by a company will require different methods of destruction. For instance, the methods used to destroy paper records will be different than those used to destroy solid state drives (SSDs). The method of destruction should be commensurate with the level of sensitivity of the document and data itself. It is Information Technology’s (IT) responsibility to ensure all users are properly informed of the enterprise’s data disposal procedures. This must be accomplished by maintaining documentation, making said documentation available to users, and ensuring users know where to find the documentation. IT should also consider training users on data disposal procedures during user awareness training. Whenever possible, the enterprise should ensure that contracts with third party services providers include clauses to destroy all company data at the request of the enterprise.

# Data Management Policy Template

## Purpose

Managing data within an enterprise includes data classification, inventory, handling, retention, and disposal. The *Data Management Policy* provides the processes and procedures for governing data within the enterprise. This includes creating a data inventory and classifying data based on sensitivity. Additionally, procedures for securely protecting data from unauthorized access or modification alongside appropriate for methods for how users should handle their data during their day-to-day work activities. Finally, authorized methods to destroy and remove data from the enterprise are discussed.

## Responsibility

* The IT business unit is responsible for managing the enterprise’s data as this information is housed on workstations and servers primarily maintained by IT. Information owners are responsible for coordinating data maintenance activities with IT.
* Users have the responsibility to protect data associated with their role from unauthorized access and disclosure. IT is responsible for informing all users of their responsibilities associated with protecting data entrusted to them.

## Exceptions

Exceptions to this policy are likely to occur. Requests for exception must be made in writing and must contain:

* The reason for the request,
* Risk to the enterprise of not following the written policy,
* Specific mitigations that will not be implemented,
* Technical and other difficulties, and
* Date of review.

## Policy

**Data Acquisition**

There are no IG1 safeguards that support this portion of the data management process.

**Data Inventory**

1. IT must conduct an inventory of data on an annual basis.
   1. All sensitive data must be marked accordingly in the data inventory.
   2. A data owner must be associated with all data tracked within the inventory.
   3. Data with specific data retention needs must be labeled accordingly.
2. All data owners are required to contact IT upon the creation of, or obtaining, sensitive data to ensure the data is tracked within the data inventory.

**Data Classification**

1. IT must establish and enforce labels for sensitive data.
2. IT must review data classification labels and their usage on an annual basis.

**Data Protection**

1. IT must configure access control lists on enterprise assets in accordance with user’s need to know. This is to include laptops, smartphones, tablets, centralized file systems, remote file systems, databases, and all applications.
2. Sensitive data must be encrypted on all user devices.

**Data Handling**

1. IT must develop and maintain a written data retention plan.
   1. All data and documents must be preserved for the appropriate amount of time as dictated by regulatory, legal, and business requirements.

**Data Disposal**

1. IT, or other authorized parties, must destroy data that have outlasted their specified retention timeframes.
2. All users are required to contact IT before disposing of sensitive data.
3. Non-sensitive data may be disposed of without speaking to IT via common destruction methods (e.g., trash, commonplace deletion from a computer system).
4. Sensitive data destruction must be performed in a manner that preserves confidentiality.
   1. Reports, correspondence, and other printed media:
      1. Shredding – Documents must be shredded using IT approved cross-cut shredders,
      2. Shredding Bins – Disposal must be performed using locked bins located on-site using an IT approved shredding service, or
      3. Incineration – Materials are physically destroyed using an IT approved incineration service.
   2. Portable Media (e.g., Solid State Drives (SSDs), digital video discs (DVDs), universal serial bus (USB) data storage devices):
      1. Physical Destruction – Complete destruction of media by means of shredding, crushing, or disassembling the asset and ensuring no data can be recovered.
   3. Hard Disc Drives (HDDs) and other magnetic media to include printer and copier hard-drives:
      1. Overwriting – Using a program to write binary data sector by sector onto the media, or
      2. Physical Destruction – Crushing, disassembling, or degaussing the asset to ensure no data can be extracted or recreated.
   4. Tape Cartridges
      1. Degaussing – Using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state, or
      2. Physical Destruction – Complete destruction of the tapes.
   5. Third-party service provider systems (e.g., cloud services) must be disposed of by first requesting the appropriate methods to permanently delete data stored in their systems, and then performing those actions according to the received instructions.
5. All destruction of data must be logged in the data inventory, when applicable.
   1. IT must obtain proof of destruction if using a third-party disposal contractor.

Revision History  
   
Each time this document is updated, this table should be updated  
.

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Revision Date | Revision Description | Name |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Appendix A: Acronyms and Abbreviations

|  |  |
| --- | --- |
| CIS | Center for Internet Security |
| CIS Controls | Center for Internet Security Critical Security Controls |
| COTS | Commercial-off-the-shelf |
| DVD | Digital Video Discs |
| GDPR | General Data Protection Regulation |
| HDD | Hard Disc Drives |
| IaaS | Infrastructure as a Service (IaaS) |
|  |  |
| IG | Implementation Group |
| IoT | Internet of Things |
|  |  |
| IT | Information Technology |
| PII | Personal Identifiable Information |
| SSD | Solid State Drives |
| SSN | Social Security Number |
| USB | Universal Serial Bus |

# Appendix B: Glossary

|  |  |
| --- | --- |
| Asset | Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).  Source: [Asset(s) - Glossary | CSRC (nist.gov)](https://csrc.nist.gov/glossary/term/asset) |
| Asset inventory | An asset inventory is a register, repository or comprehensive list of an enterprise’s assets and specific information about those assets.  Source: [Asset Inventory | FTA (dot.gov)](https://www.transit.dot.gov/TAM/resources/assetinventory) |
| Asset owner | The department, business unit, or individual responsible for an enterprise asset.  Source: CIS |
| Cloud environment | A virtualized environment that provides convenient, on-demand network access to a shared pool of configurable resources such as network, computing, storage, applications, and services. There are five essential characteristics to a cloud environment: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Some services offered through cloud environments include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). |
| Enterprise assets | Assets with the potential to store or process data. For the purpose of this document, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers in virtual, cloud-based, and physical environments.  Source: CIS Controls v8 |
| End-user devices | Information technology (IT) assets used among members of an enterprise during work, off-hours, or any other purpose. End-user devices include mobile and portable devices such as laptops, smartphones, and tablets as well as desktops and workstations. For the purpose of this document, end-user devices are a subset of enterprise assets.  Source: CIS Controls v8 |
| Enterprise asset identifier | Often a sticker or tag with a unique number or alphanumeric string that can be tracked within an enterprise asset inventory.  Source: CIS |
| Mobile end-user devices | Small, enterprise-issued end-user devices with intrinsic wireless capability, such as smartphones and tablets. Mobile end-user devices are a subset of portable end-user devices, including laptops, which may require external hardware for connectivity. For the purpose of this document, mobile end-user devices are a subset of end-user devices.  Source: CIS Controls v8 |
| Network devices | Electronic devices required for communication and interaction between devices on a computer network. Network devices include wireless access points, firewalls, physical/virtual gateways, routers, and switches. These devices consist of physical hardware as well as virtual and cloud-based devices. For the purpose of this document, network devices are a subset of enterprise assets.  Source: CIS Controls v8 |
| Non-computing/Internet of Things (IoT) devices | Devices embedded with sensors, software, and other technologies for the purpose of connecting, storing, and exchanging data with other devices and systems over the internet. While these devices are not used for computational processes, they support an enterprise’s ability to conduct business processes. Examples of these devices include printers, smart screens, physical security sensors, industrial control systems, and information technology sensors. For the purpose of this document, non-computing/IoT devices are a subset of enterprise assets.  Source: CIS Controls v8 |
| Physical environment | Physical hardware parts that make up a network, including cables and routers. The hardware is required for communication and interaction between devices on a network.  Source: CIS Controls v8 |
| Portable end-user devices | Transportable, end-user devices that have the capability to wirelessly connect to a network. For the purpose of this document, portable end-user devices can include laptops and mobile devices such as smartphones and tablets, all of which are a subset of enterprise assets.  Source: CIS Controls v8 |
| Remote devices | Any enterprise asset capable of connecting to a network remotely, usually from public internet. This can include enterprise assets such as end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers.  Source: CIS Controls v8 |
| Servers | A device or system that provides resources, data, services, or programs to other devices on either a local area network or wide area network. Servers can provide resources and use them from another system at the same time. Examples include web servers, application servers, mail servers, and file servers.  Source: CIS Controls v8 |
| User | Employees (both on-site and remote), third-party vendors, contractors, service providers, consultants, or any other user that operates an enterprise asset.  Source: CIS |
| Virtual environment | Simulates hardware to allow a software environment to run without the need to use a lot of actual hardware. Virtualized environments are used to make a small number of resources act as many with plenty of processing, memory, storage, and network capacity. Virtualization is a fundamental technology that allows cloud computing to work.  Source: CIS Controls v8 |

# Appendix C: Implementation Groups

As a part of our most recent version of the CIS Controls, v8, we created Implementation Groups (IGs) to provide granularity and some explicit structure to the different realities faced by enterprises of varied sizes.

**IG1**

An IG1 enterprise is small- to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

**IG2**

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information, and they can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

**IG3**

An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

If you would like to know more about the Implementation Groups and how they pertain to enterprises of all sizes, there are many resources that explore the Implementation Groups and the CIS Controls in general on our website at <https://www.cisecurity.org/controls/cis-controls-list/>.

# Appendix D: CIS Safeguards Mapping

**CIS Controls & Safeguards Covered by this Policy**

This policy helps to bolster IG1 Safeguards in CIS Control 3: Data Protection. Table 1 shows which IG1 CIS Safeguards are covered by this policy as written

Table 1 - Safeguards covered by IG1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CIS Control | Policy Statement | CIS Safeguard | | CIS Safeguard  Description |
| 3.1 | Usage of this policy constitutes meeting this Safeguard  Classification 1, 2  Disposal 4 | Establish and Maintain Data Management Process | Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | |
| 3.2 | Inventory 1, 1a-c, 2 | Establish and Maintain a Data Inventory | Establish and maintain a data inventory, based on the enterprise’s data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data. | |
| 3.3 | Protection 1 | Configure Data Access Control Lists | Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | |
| 3.4 | Handling 1, 1a, 1b, 1c | Enforce Data Retention | Retain data according to the enterprise’s data management process. Data retention must include both minimum and maximum timelines. | |
| 3.5 | Handling  1, 2, 2a, 3, 3a-3e | Securely Dispose of Data | Securely dispose of data as outlined in the enterprise’s data management process. Ensure the disposal process and method are commensurate with the data sensitivity. | |
| 3.6 | Protection 2 | Encrypt Data on End-User Devices | Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt. | |

# Appendix E: References and Resources

Center for Internet Security®

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

CIS Critical Security Controls®

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

Colorado Department of Education Retention Policy   
https://www.cde.state.co.us/dataprivacyandsecurity/sampleitpolicies

John Hopkins University for Center for Government Excellence   
<https://labs.centerforgov.org/data-governance/data-inventory/>

National Aeronautics and Space Administration   
https://nodis3.gsfc.nasa.gov/NPR\_attachments/NRRS\_1441.1A.pdf

U.S. National Park Service’s Data Management Guidelines for Inventory and Monitoring Networks   
https://irma.nps.gov/DataStore/DownloadFile/152590