Data Recovery   
Policy Template

**Critical Security Controls**

**March 2023**

# Contents

[Contents 2](#_Toc119315664)

[Acknowledgments 3](#_Toc119315665)

[Introduction 4](#_Toc119315666)

[Purpose 4](#_Toc119315667)

[Scope 4](#_Toc119315668)

[Data Recovery Lifecycle 5](#_Toc119315669)

[Further Discussion 8](#_Toc119315670)

[Data Recovery Policy Template 9](#_Toc119315671)

[Purpose 9](#_Toc119315672)

[Responsibility 9](#_Toc119315673)

[Policy 9](#_Toc119315674)

[Revision History 11](#_Toc119315675)

[Appendix A: Acronyms and Abbreviations 12](#_Toc119315676)

[Appendix B: Glossary 13](#_Toc119315677)

[Appendix C: Implementation Groups 15](#_Toc119315678)

[Appendix D: CIS Safeguards Mapping 16](#_Toc119315679)

[Appendix E: References and Resources 18](#_Toc119315680)

# 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

**Contributors:**

Tony Krzyzewski, SAM for Compliance Ltd  
Staffan Huslid, Truesec  
Diego Bolatti, Information Systems Engineer, Universidad Tecnológica Nacional (Argentina)   
Bryan Chou, CISSP, GSEC, GCED, GCIH  
Bryan Ferguson  
Gavin Willbond, SSS - IT Security Specialists  
Ken Muir  
Keala Asato  
Jon Matthies  
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

In the cybersecurity triad—Confidentiality, Integrity, and Availability (CIA)—the availability of data is, in some cases, more critical than its confidentiality. Enterprises need many types of data to make business decisions, and when that data is not available or is untrusted, then it could impact the enterprise. An easy example is weather information to a transportation enterprise. When attackers compromise assets, they make changes to configurations, add accounts, and often add software or scripts. These changes are not always easy to identify, as attackers might have corrupted or replaced trusted applications with malicious versions, or the changes might appear to be standard-looking account names. Configuration changes can include adding or changing registry entries, opening ports, turning off security services, deleting logs, or other malicious actions that make a system insecure. These actions do not have to be malicious; human error can cause each of these as well. Therefore, it is important to have an ability to have recent backups or mirrors to recover enterprise assets and data back to a known trusted state.

## 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 Recovery Policy* is meant as a “jumping off point” for enterprises that need help drafting their own enterprise data recovery 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 11 states:

**Control 11 – Data Recovery**

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

To support this Safeguard, it is important for an enterprise to develop a *Data Recovery Policy*. This document may include detailed steps for planning, taking backups, testing them, and actually recovering from an incident. Additionally, there should also be a portion of the policy 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 recovery data in the enterprise and the implementation of Safeguards in this CIS Control.

## 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 Recovery Lifecycle

For the safety and longevity of the enterprise, data recovery should not be left to a haphazard, slow-moving process that gets done when it’s done. In order to ensure that an enterprise can quickly recover from an incident and continue with its mission, a *Data Recovery Policy* must be put into place. Shown below in Figure 1 are the high-level “steps” of the *Data Recovery Lifecycle*, followed by a detailed description of what each step entails.

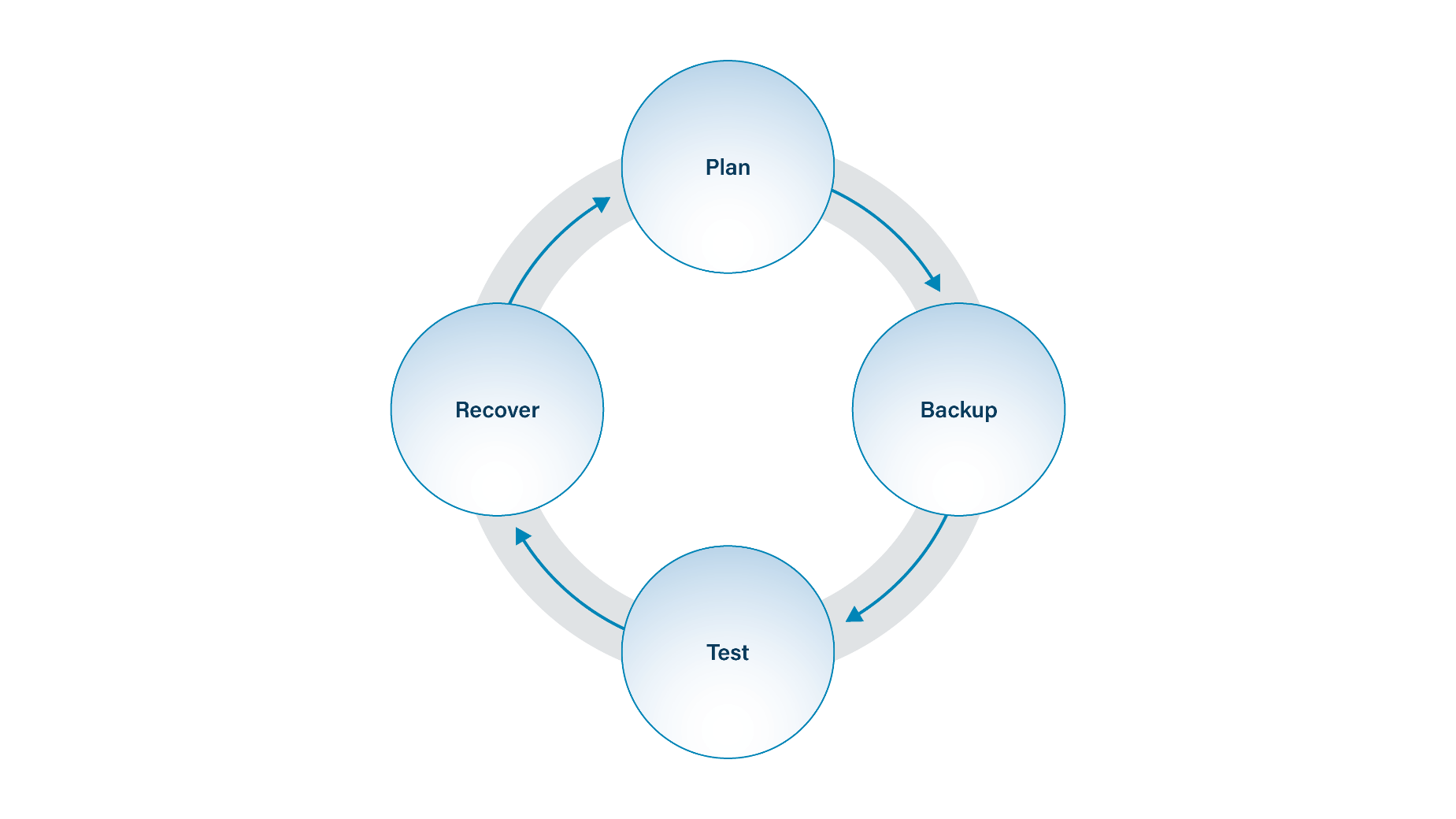


Figure 1. Data Recovery Lifecycle

* **Plan** – Create a detailed course of action to handle an overall backup strategy.
* **Backup** – Take backups from enterprise assets and transferring them to other data storage locations.
* **Test** – Ensure that the backup strategy is functioning as planned. This includes ensuring that the intended data is appropriately stored and is recoverable within the timeframes established by the data recovery plan.
* **Recover** – Execute the plan for recovery plan and get the right data back into the hands of the enterprise. Also feeds back into the planning phase.

**Plan**

One of the primary aspects of recovery planning is understanding what your recovery objectives are. Essentially, what data and enterprise assets are most important to your enterprise’s mission and how quickly does your enterprise need systems and their data at operational status. Meeting large, complex, and quick continuity objectives will likely require much planning and resources to meet. Data owners outlined in the *Data Management Policy* must be consulted to understand any impacts on data recovery. The *Enterprise Asset Inventory* and *Data Asset Inventory* can be used to help guide these prioritization discussions, since these two inventories will contain what data is already labeled most sensitive to an enterprise’s success and what assets that data resides on. These assets and data should be plainly laid out in the data recovery plan and should include backups for data stored in third-party service provider infrastructure, such as cloud platforms. Cloud service providers (CSPs) often stipulate that they do not own or are responsible for the data housed on their platforms, meaning that if the data is lost; it may be lost indefinitely. It is best to double-check with the CSP prior to onboarding to ensure that this is in-line with the enterprise’s policies.

Data recovery planning should also include the types of data storage to be used for backup purposes, where that data will geographically reside once backed up, and necessary security controls to be applied to that data to protect it from unauthorized access. Cloud storage for data backups is an adequate solution, but enterprises should verify that the data is actually stored elsewhere. Even if cloud storage is used as a primary backup strategy, there needs to be a plan for network isolated, offsite backups. The reason for this is twofold: 1) preventing ransomware that enters the network from encrypting backups and 2) preventing fires or other natural disasters from destroying backups.

**Backup**

This part of the data recovery lifecycle includes taking data from enterprise assets and storing this data elsewhere. A backup is a duplicate of a computer system’s data, but different types and degrees of backups exist. A backup is commonly viewed as a small collection of a system’s overall data. Often only a few important folders are backed up, such as containing photos, receipts, contracts, or tax information. This data may be stored on another computer system, external hard drive, removable media, or cloud service. This strategy is insufficient for protecting an enterprise. Instead, a complete system image is a snapshot of all data and settings on a system, is preferred. Flavors of backups include incremental, differential, or complete.

If a system is breached by an attacker, infected with malware, or involved in an accident (e.g., fire, flood), it often takes a long time to bring a system or network back online. This could include reinstalling and reconfiguring all the enterprise systems and applications. Complete system backups rectify this issue by backing up not just important folders, but by backing up the entire computer, which can be pushed to new systems. Although this approach is a more complex solution, it makes recovery from a disaster or computer incident significantly faster. Backups protect against many malware types including ransomware and destructive malware. Using tools and service to perform automated backups is now commonplace and is an activity worth the time to setup and manage.

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 essentially everywhere nowadays including 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 data will be available to be stolen on enterprise assets. Data retention schedules within the *Data Management Policy* should also consider the data contained within backups, as this data may not need to be saved and archived for an ill-defined amount of time. 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 data. Certain laws may specify timeframes that enterprises must keep data safe or mandate specific methods of destruction.

**Test**

Testing that a backup exists, was properly taken, and that the data within can be successfully restored is essential to a successful restoration. This ensures that, if needed, the backups will be able to restore what has been corrupted or destroyed. Too often backups are untested and can’t actually be restored in times of crisis. IT should develop testing procedures to ensure that backups taken can be restored and used without excessive time and resources. The testing process should ensure that all parties with recovery responsibilities within IT understand the prioritized recovery objectives.

**Recover**

As part of data recovery planning, enterprises should ensure that lines of communications exist between individuals charged with recovery activities and leadership roles. Additionally, granular milestones for data recovery objectives should be created to help show progress and divide recovery activities into more manageable chunks. Once an incident occurs that necessitates recovery, the data recovery planshould be put into action and implemented just as it was tested and validated. The data recovery team should work to improve the data recovery plan after an incident in order to continuously better the plan. Data recovery teams should proceed with caution when leveraging data that was touched by malicious attackers. This data may have been subtly modified or “poisoned” in some way. It may be best to recover from data untouched by attackers. Recovery planning and communication should be considered as part of the *Incident Response Policy*.

# Further Discussion

**Ransomware and Destructive Malware**

Over the past few years, ransomware (a subset of malware) has gained popularity in plaguing enterprises. There are several ransomware types. The most popular form of ransomware uses cryptography to block access to a system’s data via encryption, preventing enterprises from accessing their own data and requiring money to obtain access to the data. This type of ransomware requires affected enterprises to pay money in order to regain access to their data. Other ransomware types may instead block access and never provide it ever again, called locker ransomware or destructive malware. Double extortion ransomware has also gained popularity in the past few years, where attackers deploy ransomware to encrypt the enterprise’s data and additionally threaten to exfiltrate the enterprise’s data. This is a tactic used by attackers to try and scare enterprises into paying the ransom. In any of these scenarios, if the data is never provided back, it is considered destructive malware.

Besides user education and antivirus software, one of the best ways to recover from the impact of ransomware is backing up data to another system before there is a problem. But backups alone would not completely prevent this malware from accomplishing its goals. Typical backups may be connected to another system or network, meaning backup data can still be attacked. Therefore, regular backups should be stored in an unconnected, off-the-network, manner. Keeping offline backups helps enterprise’s recover and restore systems when ransomware or destructive malware hits a system. A common way for this malware to get into a network is to be installed via email attachments or drive-by downloads from websites. Both of these types of malware have impacted law enforcement, hospitals, governments, and academic institutions and cost millions of dollars to recover. Leveraging the guidance within the CIS Controls will help reduce the risk of ransomware through improved cyber hygiene, as attackers usually use older or basic exploits on insecure systems.

**Replication vs Backup**

Backing up data and data replication are two separate processes, and it is worthwhile to understand the distinction between them. Data backups will ensure that a second copy of data exists elsewhere within an enterprise. Best practice for data backups ensures that at least one off-network backup of all critical data is available at all times. Data backups typically represent discrete moments in time when the data was copied from one device to another device or storage medium. Backups may be stored on tape, hard drives, cloud infrastructure, or a specialized storage appliance. If an incident occurs after a computer incident or natural disaster, all data since the last backup may be lost.

In contrast to data backups, data replication provides significant gains in reliability and uptime. In the instance of replication, data replication is the “process of writing data to two separate locations.[[1]](#footnote-1) Data replication is often configured to occur in real time in order to keep the most up-to-date available to the enterprise in the event of an incident. This is often used as a way to keep a disaster recovery hot site up and running providing resiliency against computer incidents and natural disasters. Data replication often requires additional infrastructure and resources in order to function, but any hot sites can be operational in minutes after an incident.

While data replication may have certain advantages over data backups, this does not mean that data backups are not worth the effort. Any sort of backup process is better than none, especially with the continuous ransomware issues plaguing computer networks throughout the world. It’s common for enterprises to begin with data backups and move to a more advanced process over time.

**Cloud-Based Backup Strategies**

Cloud-based storage strategies are becoming more commonplace with the heavy reliance on cloud platforms in general. There’s a wide array of recovery features offered by the large cloud platforms, with some being offered for free whereas other features may be offered with additional cost such as sophisticated data analytics and integration with other technology that an enterprise may be leveraging. There are two models that are often discussed with backing up data: Software as a Service (SaaS) and Platform as a Service (PaaS). In SaaS models, enterprises leverage an application or capability that a cloud platform is offering. With PaaS scenarios, an enterprise would leverage the underlying cloud infrastructure to build tools and services with the technology the cloud service provider makes available.

# Data Recovery Policy Template

## Purpose

Proper planning will help an enterprise recover from different types of cybersecurity events or natural disasters in a timely manner. This *Data Recovery Policy* provides an overarching strategy for governing the backup and recovery of data within the enterprise. This includes creating a detailed data recovery process to ensure data is backed up on the correct assets. This process should be documented and be quickly available in case an incident occurs. Additionally, procedures for securely protecting data from unauthorized access or modification alongside appropriate methods for how users should handle their data during their day-to-day work activities.

## Responsibility

This policy is applicable to all users and IT assets. Specifically,

* The IT business unit is responsible for a majority of data recovery functions.
* Users are responsible for ensuring their enterprise data is appropriately backed up in accordance with enterprise requirements.

## Policy

**Plan**

1. A process for performing data recovery activities must be established.
   1. This process must be documented and approved.
   2. At a minimum, the data recovery process must be reviewed on an annual basis or following significant changes within the enterprise.
   3. IT must identify personnel to handle specific aspects of the data recovery process.
2. IT must identify the appropriate data to back up.
   1. IT must leverage the data inventory in order to assist with this identification process.
   2. Data owners must be consulted to understand the sensitivity of enterprise data in accordance with the data management process.
3. IT must analyze if any cloud service providers used by the enterprise are effectively backing up enterprise data, and if that data must be considered within the enterprise *Data Recovery Plan*.

**Backup**

1. IT must backup data according to the documented data recovery process.
2. Automated tools must be used to meet data backup objectives.
   1. Automated backups must be performed on a weekly basis, or more frequently.
3. Data should be retained in accordance with the data retention schedule outlined in the *Data Management Policy*.
4. Access controls must be used to prevent backups from being accessed or modified in an unauthorized manner.
5. Where practical, ensure all backups are deleted in accordance with the enterprise data destruction requirements of the *Data Management Policy*.
6. IT must maintain offsite backups of enterprise data.
   1. This data must not be directly accessible from a network.

**Test**

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

**Recover**

1. During an incident, IT must leverage the data recovery plan to restore data and functionality in a prioritized manner.
2. Ensure the incident response team is included in the data recovery process.
3. The incident response plan must be activated.

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

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

# Appendix A: Acronyms and Abbreviations

|  |  |
| --- | --- |
| CIA | Confidentiality, Integrity, and Availability |
| CIS | Center for Internet Security |
| CIS Controls | Center for Internet Security Critical Security Controls |
| COTS | Commercial-off-the-shelf |
| CSP | Cloud Service Provider |
| GDPR | General Data Protection Regulation |
| ICS | Industrial Control System |
| IG | Implementation Group |
| IT | Information Technology |
| PaaS | Platform as a Service (PaaS) |
| SaaS | Software as a Service |
| SIEM | Security Information and Event Management |

# 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) |
| 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 |
| 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 |
| 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 |

# 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 11: *Data Recovery*. Table 1 shows which IG1 Safeguards are covered by this policy as written.

Table - Safeguards covered by IG1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CIS Control | Policy Statement | CIS Safeguard | CIS Safeguard  Description | |
| 3.1 | Plan 2b | Establish and Maintain a Data Management Process | Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | |
| 3.3 | Backup 4 | 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 | Backup 3 | Enforce Data Retention | | Retain data according to the enterprise’s data management process. Data retention must include both minimum and maximum timelines. |
| 3.6 | Backup 4 | 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. |
| 11.1 | Plan  1, 1a, 1b, 2, 2a, 3  Backup 1  Recover 1 | Establish and Maintain a Data Recovery Process | | Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |
| 11.2 | Backup 2, 2a | Perform Automated Backups | | Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data. |
| 11.3 | Backup 4 | Protect Recovery Data | | Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements. |
| 11.4 | Backup 6, 6a | Establish and Maintain an Isolated Instance of Recovery Data | | Establish and maintain an isolated instance of recovery data. Example implementations include version controlling backup destinations through offline, cloud, or off-site systems or services. |

# Appendix E: References and Resources

Center for Internet Security®

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

CIS Critical Security Controls®

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

US-CERT: Ransomware - What It Is and What You Can Do   
<https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf>

Ransomware Guide (CSA / MS-ISAC)  
<https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf>

UK NCSS: Mitigating Malware   
<https://www.ncsc.gov.uk/guidance/mitigating-malware>

NIST National Cybersecurity Center of Excellence: Data Integrity <https://www.nccoe.nist.gov/sites/default/files/library/sp1800/di-nist-sp1800-11-draft.pdf>

NIST SP 800-34 Rev 1: Contingency Planning Guide for Federal Information Systems   
<https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final>

NIST SP 800-209: Security Guidelines for Storage Infrastructure  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf>

Microsoft Backup and Restore: Built-in backup utility tool  
<https://support.microsoft.com/en-us/help/17127/windows-back-up-restore>

Amanda Network Backup  
<http://www.amanda.org>

Bacula  
<http://blog.bacula.org>

Veracrypt  
<https://www.veracrypt.fr/en/How%20to%20Back%20Up%20Securely.html>

EaseUS  
<https://www.easeus.com/backup-software/tb-free.html>

1. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf> [↑](#footnote-ref-1)