Account and Credential Management Policy Template

**CIS Critical Security Controls**

**November 2022**

# Contents

[Contents 2](#_Toc117435005)

[Acknowledgments 3](#_Toc117435006)

[Introduction 4](#_Toc117435007)

[Purpose 4](#_Toc117435008)

[Types of Accounts & Credential Management 4](#_Toc117435009)

[Types of Credentials 5](#_Toc117435010)

[Scope 5](#_Toc117435011)

[Account & Credential Management Lifecycle 6](#_Toc117435012)

[Account & Credential Management Policy Template 9](#_Toc117435013)

[Purpose 9](#_Toc117435014)

[Responsibility 9](#_Toc117435015)

[Exceptions 9](#_Toc117435016)

[Policy 9](#_Toc117435017)

[Revision History 12](#_Toc117435018)

[Appendix A: Acronyms and Abbreviations 13](#_Toc117435019)

[Appendix B: Glossary 14](#_Toc117435020)

[Appendix C: Implementation Groups 16](#_Toc117435021)

[Appendix D: CIS Safeguards Mapping 17](#_Toc117435022)

[Appendix E: References and Resources 19](#_Toc117435023)

# 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:**

Tony Krzyzewski, SAM for Compliance Ltd  
Jon Matthies  
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  
Robin Regnier, 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

Accounts and credentials such as passwords are how we access phones, tablets, workstations, and web applications. Each of these accounts can be used to gain unauthorized access into an enterprise’s walled garden to steal data. There are many ways to covertly obtain access to accounts such as weak passwords, old accounts from a fired employee, or passwords involved in a data breach for a separate company that are also used on your systems. There are multiple types of accounts that often need to be managed.

## Purpose

The CIS Critical Security Controls® (CIS Controls®) describe multiple policies that an enterprise should have in place. That includes a set of policies to cover how accounts and credentials are managed in the enterprise, and other access control related functions. This policy is meant as a “jumping off point” for enterprises needing to draft their own policies. 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, Controls 5 and 6 state:

**Control 5 – Account Management**

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

**Control 6 –Access Control Management**

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

To support this Safeguard, it is important for an enterprise to develop policies and processes to control access in the enterprise. This document supports the development of those processes in accordance with the CIS Controls.

## Types of Accounts & Credential Management

The CIS Controls cover a broad array of authentication, authorization, and account management functions. Multiple types of accounts exist, and all need to be managed in some manner. These types of accounts can include:

* Administrative accounts: Also known as superuser, privileged, or root accounts, these accounts have extensive privileges to control operating systems, applications, and platforms.
* User accounts: These accounts are normally privileged accounts used by employees and contractors to perform their work duties.
* Vendor accounts: Accounts created by the vendor of a technology, such as a firewall or cloud platform. These accounts may, or may not, be administrative accounts. They are often pre-installed, and the usernames and passwords may be widely known, leading to an access vulnerability.
* Default accounts: These accounts are often pre-installed, and the usernames and passwords may be widely known, leading to a backdoor. They may be vendor accounts, yet they may also be accounts for any user to leverage.

## Types of Credentials

* Passwords: Memorized text that may include numbers, special characters, and capital letters. For this document, personal identification numbers (PINs), passwords, and passphrases are all categorized as “passwords”.
* Software authenticator: This password or PIN will be used one time and may be sent via a short message service (SMS) or shared within an app. Additionally, this method of authentication may simply require an interaction between the user and their device, such as selecting “Yes this is me” within a mobile application. There are many different types of software authenticators and this is continuing to evolve as technology changes.
* Physical one-time credential: These are physical devices that often provide users with a rotating PIN. The most common example is an RSA token.
* Physical Badge: These badges are often worn and are used to enter and exit buildings. The badge may provide a picture of the employee also be able to communicate wirelessly with a physical access control system or may contain additional credentials for a user, such as a cryptographic key.
* Biometrics: Mobile devices make leveraging biometric credentials such as the face, retina, or fingerprint much more readily available.

## 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.

# Account and Credential Management Lifecycle

Just like assets, accounts and credentials must be tracked to ensure they are being used in a proper and authorized manner. This is due to the fact that they are the primary entry point into the enterprise network. Additionally, accounts and credentials must be securely created and provisioned to users in the enterprise. Credentials must be of a certain strength in order to be realistically secure in today’s threat environment since old, weak, or even forgotten credentials are a prime candidate as a means for unauthorized access. Figure 1 shows the overall lifecycle of how accounts and credentials are created, used, and ultimately revoked.

A picture containing diagram

Description automatically generated

Figure 1. Account and Credential Management Lifecycle Diagram

* **Onboarding** – This process brings new users in the enterprise. Their identity is verified to ensure they are who they say they are.
* **Account Creation** – Once it is deemed that a new user will join the enterprise, accounts must be created for them. These accounts may be stored in Active Directory, but additional accounts for specific applications and services may also be necessary. These accounts will have permissions assigned to them based on their role.
* **Credential Creation and Issuance** – Passwords, badges, and any other credentials needed for a user to leverage their accounts in the workplace need to be created and provided to the user.
* **Account and Credential Usage** – Users will leverage their accounts and credentials to access work resources to perform their job duties.
* **Monitor** – Accounts must also be tracked and monitored to ensure they are being used appropriately.
* **Modify Access** – People may leave the company, go on extended medical leave, or simply change jobs within the enterprise. The permissions afforded to an account when a user starts with the company are rarely the exact set of permissions they have when they leave the company.
* **Account Termination** – When employees leave the enterprise, their credentials should be revoked, and they should no longer have access to their accounts.

**Onboarding**

An identity can be thought of as a set of attributes uniquely describing a person, device, or other entity within a given context. In the case of onboarding, creating an account for an individual is how identities are created for new users and contractors. Yet it is important to ensure that people are actually who they say they are before they are given enterprise access. Said more succinctly; enterprises must verify users before they are employed. Public institutions like federal and state, local, tribal, and territorial (SLTT) governmental agencies in the United States will often verify biometric and other records against law enforcement and other governmental databases. It is common for private employers to perform credit, criminal, and other background checks to verify identity.

**Account Creation**

Once identities have been verified for new users, accounts are then created for them. Accounts essentially act as the *de facto* “identity” within the enterprise, and are often stored in Directory Services, such as Microsoft Active Directory. Yet it is uncommon for Active Directory to be able to support all accounts that are needed. Most enterprises leverage third-party applications that may or may not integrate with Active Directory. Additionally, cloud applications often require accounts and these are often separate accounts and are not necessarily associated with accounts made and used within the enterprise. Some third-party services and platforms will support identity federation, meaning no new accounts will need to be created.

Once accounts are created for any platform, they should be placed into the account inventory. This inventory is a record of all accounts in use for any and all software and other applications used throughout the entire enterprise. Although this can be difficult, this inventory should be kept up to date. This inventory will be used as the foundation for managing a user’s identity throughout the company, from gaining new privileges to being decommissioned or removed. Without this inventory, it’s much easier for accounts to be forgotten and left active. A common method used for threat actors to gain access to an enterprise is via impersonation, using legitimately created accounts.

**Credential Creation and Issuance**

The purpose of credentials is to validate an identity. Examples of credentials can be found under *Types of Credentials* within this document. Note that the security strength of credentials are not created equal. Some credentials are stronger, or more trustworthy, than others. Enterprises must make an early decision on which credentials they will be issuing to users. Additionally, combinations of different types of credentials enables multifactor authentication, which should be the default method of authenticating in many enterprise applications.

Passwords are ubiquitous in modern society and are often the most common form of credential used by an enterprise. If you have an account on a computer system, there will likely be at least one password that will need to be managed. CIS provides a separate [password policy guide](https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide) that can help enterprises make sound decisions on password strength and usage.

Finally, how credentials are provisioned to users makes a difference in how secure they are. Provisioning credentials to users physically in-person has a positive impact on their trustworthiness, meaning that giving credentials to users in-person is generally considered more secure. Remotely providing credentials to users is sometimes necessary, such as with full-time remote users or providing credentials via a user’s mobile device. When this is done, suitable security precautions (e.g., encryption) should be taken to protect the credential in transit.

**Account and Credential Usage**

The authentication process uses identities and credentials to verify a user’s identity claims. Protocols are used to perform the authentication process with networks and computers. Some protocols are stronger than others and modern, secure protocols should be used whenever possible. Once authentication is successful, a user is provided rights and privileges to enterprise resources. Remote authentication, such as authenticating via enterprise credentials over a network, generally requires stronger types of authentication. Multifactor authentication should be used in these instances.

**Monitor**

As users arrive and leave the enterprise, it is best to periodically check the status of the user accounts in your account inventory. Some accounts will sneak under the radar and still retain rights and permissions to sensitive data long after the user is gone. Dormant and forgotten accounts are prime targets for attackers to find and use to breach an enterprise network.

Administrative accounts are an important subset of accounts to focus on and secure. These accounts have the ability to completely shut down an enterprise’s network if misused. Therefore, their activity and use should be monitored and when an administrator leaves the enterprise these accounts should be quickly deactivated or removed. Additionally, it is important to ensure administrator permissions are not provided to an administrator’s normal user account. This can cause security-relevant incidents and accidents where an administrator’s system is infected with malware and then the malware executes with super-user privileges.

**Modify Access**

Employees may leave the company, go on extended medical leave, or simply change jobs within the enterprise. The permissions afforded to an account when a user starts with the company are rarely the exact set of permissions they have when they leave. As users leverage their accounts, they will often require new permissions to access new resources for new projects and to access new technology and applications that the enterprise begins using. Users change roles or are added to new projects quite often, so this can be a large, ongoing process.

**Account Termination**

When users leave the enterprise, their credentials should be revoked and they should no longer have access to their accounts. This should happen as soon as practical after they leave the enterprise so that the user cannot abuse their access. Some enterprises even revoke access before a user is terminated so there is no opportunity for abuse to occur. It is important to have a written process for account and credential revocation so that when the situation arises, administrators and other relevant personnel know what do in the moment. It’s commonplace for accounts to disabled instead of deleted to preserve an audit trail. Directly removing the accounts may create unreadable portions in logfiles and other parts of the audit trail.

# Account and Credential Management Policy Template

## Purpose

Account and credential management is the process of creating, provisioning, using, and terminating accounts and credentials in the enterprise. The *Account and Credential Management Policy* provides the processes and procedures for governing accounts and credentials.

## Responsibility

* The IT business unit is responsible for all account and credential management functions. This information is relayed to other business units within the enterprise such as finance, accounting, and cybersecurity as required or needed. IT is responsible for informing all users of their responsibilities in the use of any accounts and credentials assigned to them.
* Users are responsible for using their accounts in a manner consistent with enterprise policy.

## 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

**Onboarding**

1. IT must maintain procedures for modifying access, permissions, and roles to user accounts.
2. Newly created accounts must be represented within this process.
3. Changing user roles must be included in this process.
4. The permissions granting process must enforce the principle of least privilege.
5. Unnecessary default or generic accounts must be changed before a new system is deployed into the enterprise.

**Account Creation**

1. IT must develop procedures for creating accounts and assigning privileges.
2. Administrator privileges must only be provided to administrative accounts.
   1. Administrator and privileged accounts must only be used for appropriate installation and maintenance tasks; not for daily use.
   2. Administrator accounts must be unique and assigned to a specific individual, unless technically constrained by a system or application.
3. It is the responsibility of IT to maintain an account inventory.
4. At a minimum the account inventory must contain the following data for each account:
5. Person's name
6. Account name
7. Date of employment start and stop
8. Business unit
9. Account status (i.e., enabled, disabled)
10. All enabled accounts within the inventory must be regularly validated once a quarter, or more frequently

**Credential Creation and Issuance**

1. All passwords must be unique.
2. Passwords created by users must not also be used for personal accounts.
3. Passwords must not be shared by users.
4. Passwords created for use with multifactor authentication must be at a minimum 8 characters long.
5. Passwords created for use without multifactor authentication must be at a minimum 14 character long.

**Account and Credential Usage**

1. All users must use multifactor authentication to access externally facing applications.
2. All users must use multifactor authentication to access applications hosted by a third-party service provider, where supported.
3. All remote users must use multifactor authentication to access internal systems and applications.
4. Multifactor authentication is required for all administrative accounts on all enterprise assets, whether managed on-site or through a third-party provider.
5. All default user passwords must be changed at the first login.

**Monitor**

There are no IG1 safeguards that support this portion of the account and credential management process.

**Modify Access**

1. All user accounts that have not been accessed within 45 days of creation must be disabled.
2. Accounts of individuals on extended leave, as defined by human resources, must be disabled.
3. The Account Creation and Account Termination procedures must include the ability to change a user’s role.

**Account Termination**

1. IT must develop procedures for revoking account access.
   1. Termination of employees must be included in this process.
2. All user credentials must be revoked immediately upon employee separation.
   1. Password self-service mechanisms for users must not allow them to re-enable their own account.

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 |
| IaaS | Infrastructure as a Service (IaaS) |
| IG | Implementation Group |
| IoT | Internet of Things |
| IT | Information Technology |
| PIN | Personal Identification Number |
| SLTT | State, Local, Tribal, and Territorial |
| SMS | Short Message Service |

# 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 5: Account Management* and *CIS Control 6: Access Control Management.* 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 |
| 5.1 | Account Creation  3, 4, 5 | Establish and Maintain an Inventory of Accounts | Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person’s name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. |
| 5.2 | Credential Creation and Issuance 1, 1a, 1b, 2, 3  Account usage 5 | Use Unique Passwords | Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |
| 5.3 | Modify Access 6, 7  Account usage 5 | Disable Dormant Accounts | Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported. |
| 5.4 | Account Creation  2, 2a, 2b | Restrict Administrator Privileges to Dedicated Administrator Accounts | Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user’s primary, non-privileged account. |
| 6.1 | Onboarding  1a, 1b, 1c, 1d Account Creation 1  Modify Access 8 | Establish an Access Granting Process | Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user. |
| 6.2 | Account Termination  1, 1a, 2, 2a Modify Access 8 | Establish an Access Revoking Process | Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |
| 6.3 | Account Usage 1, 2 | Require MFA for Externally-Exposed Applications | Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. |
| 6.4 | Account Usage 3 | Require MFA for Remote Network Access | Require MFA for remote network access. |
| 6.5 | Account Usage 4 | Require MFA for Administrative Access | Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider. |

# Appendix E: References and Resources

Center for Internet Security®

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

CIS Critical Security Controls®

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