YourIT!
Your Logo Goes Here

CIS Controls v8.1 - IG1

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

Purpose

CIS Controls v8.1 defines Implementation Group 1 (IG1) as essential cyber hygiene and represents an emerging minimum standard of information security for all enterprises. IG1 is the on-ramp to the CIS Controls and consists of a foundational set of 56 cyber defense Safeguards. The Safeguards included in IG1 are what every enterprise should apply to defend against the most common attacks.

Scope

An Implementation Group 1 (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.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CIS Control 01 - Inventory and Control of Enterprise Assets

CIS Controls v8.1 - IG1	Other Requirements
CIS Control 01 Inventory and Control of Enterprise Assets	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them (CIS Control 3), and proper asset management will help identify those enterprise assets that hold or manage this critical data, so that appropriate security controls can be applied.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS1.1 - Establish and Maintain Detailed Enterprise Asset Inventory: Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

- CIS1.2 - Address Unauthorized Assets: Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

CIS Control 02 - Inventory and Control of Software Assets

CIS Controls v8.1 - IG1	Other Requirements
CIS Control 02 Inventory and Control of Software Assets	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
A complete software inventory is a critical foundation for preventing attacks. Attackers continuously scan target enterprises looking for vulnerable versions of software that can be remotely exploited. For example, if a user opens a malicious website or attachment with a vulnerable browser, an attacker can often install backdoor programs and bots that give the attacker long-term control of the system. Attackers can also use this access to move laterally through the network. One of the key defenses against these attacks is updating and patching software (CIS Control 7). However, without a complete inventory of software assets, an enterprise cannot determine if they have vulnerable software, or if there are potential licensing violations.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS2.1 - Establish and Maintain a Software Inventory: Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, decommission date, and number of licenses. Review and update the software inventory bi-annually, or more frequently.

- CIS2.2 - Ensure Authorized Software is Currently Supported : Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.

- CIS2.3 - Address Unauthorized Software: Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

CIS Control 03 - Data Protection

CIS Controls v8.1 - IG1	Other Requirements
CIS Control 03 Data Protection	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
Data is no longer only contained within an enterprise's border; it is in the cloud, on portable end-user devices where users work from home, and is often shared with partners or online services that might have it anywhere in the world. In addition to sensitive data an enterprise holds related to finances, intellectual property, and customer data, there also might be numerous international regulations for protection of personal data. Data privacy has become increasingly important, and enterprises are learning that privacy is about the appropriate use and management of data, not just encryption. Data must be appropriately managed through its entire life cycle. These privacy rules can be complicated for multi-national enterprises of any size; however, there are fundamentals that can apply to all.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS3.1 - Establish and Maintain a Data Management Process: Establish and maintain a documented 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.

- CIS3.2 - 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.

- CIS3.3 - 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.

- CIS3.4 - Enforce Data Retention: Retain data according to the enterprise’s documented data management process. Data retention must include both minimum and maximum timelines.

- CIS3.5 - Securely Dispose of Data: Securely dispose of data as outlined in the enterprise’s documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.

- CIS3.6 - 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.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

CIS Control 04 - Secure Configuration of Enterprise Assets and Software

CIS Controls v8.1 - IG1	Other Requirements
CIS Control 04 Secure Configuration of Enterprise Assets and Software	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
As delivered from manufacturers and resellers, the default configurations for enterprise assets and software are normally geared towards ease-of-deployment and ease-of-use, rather than security. Basic controls, open services and ports, default accounts or passwords, pre-configured Domain Name System (DNS) settings, older (vulnerable) protocols, and pre installation of unnecessary software can all be exploitable if left in their default state. Further, these security configuration updates need to be managed and maintained over the life cycle of enterprise assets and software. Configuration updates need to be tracked and approved through configuration management workflow process to maintain a record that can be reviewed for compliance, leveraged for incident response, and to support audits. This CIS Control is important to on-premises devices, as well as remote devices, network devices, and cloud environments.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS4.1 - Establish and Maintain a Secure Configuration Process: Establish and maintain a documented secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure: Establish and maintain a documented secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS4.3 - Configure Automatic Session Locking on Enterprise Assets: Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.

- CIS4.4 - Implement and Manage a Firewall on Servers: Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.

- CIS4.5 - Implement and Manage a Firewall on End-User Devices: Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

- CIS4.6 - Securely Manage Enterprise Assets and Software: Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.

- CIS4.7 - Manage Default Accounts on Enterprise Assets and Software: Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

CIS Control 05 - Account Management

CIS Controls v8.1 - IG1	Other Requirements
CIS Control 05 Account Management	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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.

Guidance
It is easier for an external or internal threat actor to gain unauthorized access to enterprise assets or data through using valid user credentials than through hacking the environment. There are many ways to covertly obtain access to user accounts, including: weak passwords, accounts still valid after a user leaves the enterprise, dormant or lingering test accounts, shared accounts that have not been changed in months or years, service accounts embedded in applications for scripts, a user having the same password as one they use for an online account that has been compromised (in a public password dump), using social engineering techniques to obtain a password, or using malware to capture passwords or tokens in memory or over the network. Defenders need to ensure that controls are in place to protect enterprise accounts, especially those with higher privileges.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS5.1 - Establish and Maintain an Inventory of Accounts: Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must at a minimum include user, administrator accounts, and service 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.

- CIS5.2 - Use Unique Passwords: Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.

- CIS5.3 - Disable Dormant Accounts: Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.

- CIS5.4 - 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.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

CIS Control 06 - Access Control Management

CIS Controls v8.1 - IG1	Other Requirements
CIS Control 06 Access Control Management	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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.

Guidance
Where CIS Control 5 deals specifically with account management, CIS Control 6 focuses on managing what access these accounts have, ensuring users only have access to the data or enterprise assets appropriate for their role, and ensuring that there is strong authentication for critical or sensitive enterprise data or functions. Attackers will compromise any account that will grant them access to a network, especially administrator accounts that have elevated privileges. Accounts should only have the minimal authorization needed for the role. Developing consistent access rights for each role and assigning roles to users is a best practice. Developing a program for complete provision and de-provisioning access is also important. Centralizing this function is ideal.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS6.1 - Establish an Access Granting Process: Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user.
- CIS6.2 - 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.
- CIS6.3 - 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.
- CIS6.4 - Require MFA for Remote Network Access: Require MFA for remote network access.
- CIS6.5 - 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 service provider.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

CIS Control 07 - Continuous Vulnerability Management

CIS Controls v8.1 - IG1	Other Requirements
CIS Control 07 Continuous Vulnerability Management	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Guidance
Thousands of vulnerabilities are published each year, with several more that are unknown. Cyber defenders are constantly being challenged from attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Defenders must have timely threat information available to them about: software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS7.1 - Establish and Maintain a Vulnerability Management Process: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS7.2 - Establish and Maintain a Remediation Process: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

- CIS7.3 - Perform Automated Operating System Patch Management: Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

- CIS7.4 - Perform Automated Application Patch Management: Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

References

- CIS Controls Cloud Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-cloud-companion-guide
- CIS Critical Security Controls v8 Mobile Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mobile-companion-guide
- CIS Controls v8 Internet of Things Companion Guide - - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide

Truncated Sample Document