Minimum Baseline of Cybersecurity - Have a Plan

Overview

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.

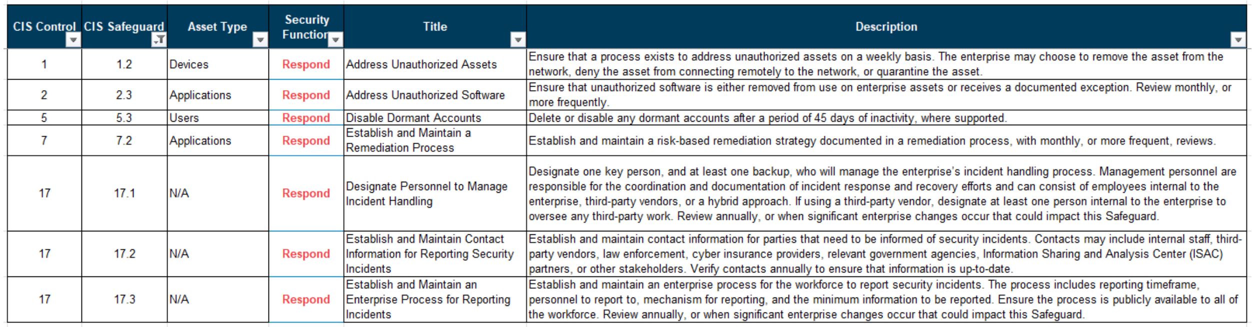
Actively manage (inventory, track and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

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.

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

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training and communications) to prepare, detect and quickly respond to an attack.

Applicable Controls



CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description
1	1.2	Devices	Respond	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.
2	2.3	Applications	Respond	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.
5	5.3	Users	Respond	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.
7	7.2	Applications	Respond	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.
17	17.1	N/A	Respond	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
17	17.2	N/A	Respond	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.
17	17.3	N/A	Respond	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Address Unauthorized Assets (1.2)

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.

Address Unauthorized Software (2.3)

Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly or more frequently.

Disable Dormant Accounts (5.3)

Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.

Establish and Maintain a Remediation Process (7.2)

Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

Designate Personnel to Manage Incident Handling (17.1)

Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, service providers, or a hybrid approach. If using a service provider, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Establish and Maintain Contact Information for Reporting Security Incidents (17.2)

Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up to date.

Establish and Maintain an Enterprise Process for Reporting Incidents (17.3)

Establish and maintain a documented enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Policy Templates for these security controls:

Acceptable Use Policy Template for the CIS Controls

This template can assist an enterprise in developing acceptable use for the CIS Controls.
Download the template

Enterprise Asset Management Policy Template for CIS Control 1

This template can assist an enterprise in developing an enterprise asset management policy.
Download the template

Software Asset Management Policy Template for CIS Control 2

This template can assist an enterprise in developing a software asset management policy.
Download the template

Account and Credential Management Policy Template for CIS Controls 5 and 6

This template can assist an enterprise in developing an account and credential management policy.
Download the template

Vulnerability Management Policy Template for CIS Control 7

This template can assist an enterprise in developing a data management policy.
Download the template

Incident Response Policy Template for CIS Control 17

This template can assist an enterprise in developing an incident response policy.
Download template

Public and Non-profit Tools That may support small business and municipalities with inventory discovery:

MassCyberCenter Incident Reporting Planning Brochure

MassCyberCenter Incident Response Planning Resources

SANS Institute Incident Handler's Handbook

National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide

ITS78: Statewide Contract for Data, Cybersecurity, and Related Audit, Compliance, and Incident Responses Services