YourIT!
Your Logo Goes Here

Kaseya Cybersecurity Fundamentals

Kaseya Cybersecurity Fundamentals - Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

Purpose

The purpose is to ensure that the organization has implemented a number of basic IT Security Controls and Practices.

Scope

This policy applies to the workforce members of organizations and third-parties who access organization information systems.

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.

Kaseya Cybersecurity Fundamentals CSF Function 1: ID - Identify

Kaseya Cybersecurity Fundamentals	Other Requirements
CSF Function 1: ID Identify	N/A

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

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Guidance
The NIST Cybersecurity Framework's Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Examples of outcome Categories within this Function include:

1. Identifying physical and software assets within the organization to establish the basis of an Asset Management program

2. Identifying the Business Environment the organization supports including the organization's role in the supply chain, and the organizations place in the critical infrastructure sector

3. Identifying cybersecurity policies established within the organization to define the Governance program as well as identifying legal and regulatory requirements regarding the cybersecurity capabilities of the organization

4. Identifying asset vulnerabilities, threats to internal and external organizational resources, and risk response activities as a basis for the organizations Risk Assessment

5. Identifying a Risk Management Strategy for the organization including establishing risk tolerances

6. Identifying a Supply Chain Risk Management strategy including priorities, constraints, risk tolerances, and assumptions used to support risk decisions associated with managing supply chain risks

Source: NIST Cybersecurity Framework - The Five Functions

https://www.nist.gov/cyberframework/online-learning/five-functions

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

Related Internal Controls

- CC1.1 - Inventories: Establish and maintain inventories of organizational systems (including hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware) throughout the respective system development life cycles.

- CC5.1 - Risk Assessment/Risk Analysis: Periodically conduct an accurate and thorough assessment of the risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of data.

  Procedure
  - Conduct a comprehensive, accurate and thorough risk assessment/HIPAA Security Risk Analysis.
  - Bring in an independent expert to perform your risk assessment without any conflict of interest.

- CC17.5 - Identify Threats: Identify and document threats, both internal and external.

  Procedure
  - Threat scanners and information sharing platforms should be used to identify activities that can take advantage of vulnerabilities.

References

- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- NIST CSF Framework (pdf) - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NIST CSF Framework (Excel) - https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx

Kaseya Cybersecurity Fundamentals CSF Function 2: PR - Protect

Kaseya Cybersecurity Fundamentals	Other Requirements
CSF Function 2: PR Protect	N/A

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

Develop and implement appropriate safeguards to ensure delivery of critical services.

Guidance
The NIST Cybersecurity Framework's Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

Examples of outcome Categories within this Function include:

1. Protections for Identity Management and Access Control within the organization including physical and remote access

2. Empowering staff within the organization through Awareness and Training including role based and privileged user training

3. Establishing Data Security protection consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information

4. Implementing Information Protection Processes and Procedures to maintain and manage the protections of information systems and assets

5. Protecting organizational resources through Maintenance, including remote maintenance, activities

6. Managing Protective Technology to ensure the security and resilience of systems and assets are consistent with organizational policies, procedures, and agreements

Source: NIST Cybersecurity Framework - The Five Functions

https://www.nist.gov/cyberframework/online-learning/five-functions

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

Related Internal Controls
- CC7.1 - Identity Management: Manage identities and credentials for authorized devices and users.

Procedure
- Provide access to resources in relation to a user's role and responsibilities. All users should be uniquely identifiable, including vendors and other third-parties.

- CC7.4 - Access Permission Management: Manage access permissions, incorporating the principles of least privilege and separation of duties.

  Procedure
  - Set up all systems to provide the least amount of privilege a user needs to perform their job function.

- CC7.6 - HR Cybersecurity Alignment: Ensure that cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).

  Procedure
  - Create formal communications processes between HR and other departments to ensure new users are properly provisioned and that terminated users are immediately denied access.

- CC7.36.1 - Multi-Factor Authentication: Require Multi-Factor Authentication enforcement on all externally exposed enterprise or third party applications, remote network access, and all Privileged accounts where supported.

  Procedure
  - The Organization Shall Enforce MFA to the greatest extent possible.

- CC8.1 - Protect Data: Ensure data-at-rest (stored) is protected.

  Procedure
  - Deploy tools and utilize processes to protect all stored data.

- CC8.3 - Ensure Adequate Capacity: Ensure there is adequate capacity to ensure availability is maintained.

  Procedure
  - Purchase systems with enough capacity, and periodically review capacity usage and foreseeable needs to prevent outages.

- CC8.4 - Protect Against Data Leaks: Protections against data leaks are implemented.

  Procedure
  - Deploy tools and utilize processes to prevent data from being transferred within or outside the organization without authorization.

- CC8.16 - Control & Limit Access: Ensure that access to systems and assets is controlled, incorporating the principle of least functionality.

  Procedure
  - Only provide the minimum level of access to devices, and use restrictions in software and cloud services, to minimize the functionality to users based on their roles and responsibilities.

- CC8.19 - Firewall Protection: Ensure that firewalls with active intrusion prevention protect the perimeter of the network.

  Procedure
  - Deploy business-class firewall protection to all devices, including remote systems, and maintain current firmware and subscriptions for security services.

- CC9.2 - Perform & Control Maintenance & Repairs: Ensure maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.

  Procedure
  - Hackers have impersonated maintenance and repair personnel. Make sure that maintenance and repair personnel and only performing required tasks on authorized equipment.

- CC14.12 - Data Backup Plan: Write a comprehensive data backup plan that identifies the locations of all business-critical and regulated data, and the detailed process used to create and test backups.

  Procedure
  - Write a backup plan identifying the location of all data, how it is backed up, the frequency of backups, where backups are stored, and how they are tested.

- CC16.1 - Workforce Training: Implement workforce training that covers all required policies and procedures.

  Procedure
  - Conduct workforce training at the time of hire and regularly afterwards. Ensure all workforce members, including executives and contractors, complete their training.
  - Supplement packaged training programs with customized training focused on your unique environment, for example, the keyword that should be entered in an email subject line to send an encrypted message. Include requirements for security of work-from-home environments, secure connecting from public networks, etc.

References

- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- NIST CSF Framework (pdf) - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NIST CSF Framework (Excel) - https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx

Kaseya Cybersecurity Fundamentals CSF Function 3: DE - Detect

Kaseya Cybersecurity Fundamentals	Other Requirements
CSF Function 3: DE Detect	N/A

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

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Guidance
The NIST Cybersecurity Framework's Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.

Examples of outcome Categories within this Function include:

1. Ensuring Anomalies and Events are detected, and their potential impact is understood

2. Implementing Security Continuous Monitoring capabilities to monitor cybersecurity events and verify the effectiveness of protective measures including network and physical activities

3. Maintaining Detection Processes to provide awareness of anomalous events

Source: NIST Cybersecurity Framework - The Five Functions

https://www.nist.gov/cyberframework/online-learning/five-functions

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

Related Internal Controls
- CC1.5 - Baseline Configurations: Establish and maintain baseline configurations of organizational systems (including hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, firmware, and reporting requirements) throughout the respective system development life cycles.

- CC17.1 - Vulnerability Scans: Scan for vulnerabilities and encryption status in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

  Procedure

    - Regularly scan for vulnerabilities. In 2020, 50 new high-risk vulnerabilities were identified every day, meaning that scans should be run at least monthly to provide adequate protection.

- CC18.12 - Malicious Code Detection: Ensure that malicious code is detected.

  Procedure
    - Utilize multiple systems to detect malicious code in software, devices, cloud services, and files.

- CC18.15 - Monitoring: Ensure that monitoring the network for unauthorized personnel, connections, devices, and software is performed.

  Procedure
    - Use a multi-layered approach to identify unauthorized personnel, connections, devices, and software.

- CC18.19 - Improve Detection Processes: Ensure that detection processes are continuously improved.

  Procedure
    - Because vulnerabilities and threats change, review your detection processes to ensure they are effective against current threats.

References

- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- NIST CSF Framework (pdf) - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NIST CSF Framework (Excel) - https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx

Kaseya Cybersecurity Fundamentals CSF Function 4: RS - Respond

Kaseya Cybersecurity Fundamentals	Other Requirements
CSF Function 4: RS Respond	N/A

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

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Guidance
The NIST Cybersecurity Framework's Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

Examples of outcome Categories within this Function include:

1. Ensuring Response Planning process are executed during and after an incident

2. Managing Communications during and after an event with stakeholders, law enforcement, external stakeholders as appropriate

3. Analysis is conducted to ensure effective response and support recovery activities including forensic analysis, and determining the impact of incidents

4. Mitigation activities are performed to prevent expansion of an event and to resolve the incident

5. The organization implements Improvements by incorporating lessons learned from current and previous detection / response activities

Source: NIST Cybersecurity Framework - The Five Functions

https://www.nist.gov/cyberframework/online-learning/five-functions

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

Related Internal Controls
- CC17.12 - Newly-Identified Vulnerabilities: Ensure that newly identified vulnerabilities are mitigated or documented as accepted risks.

  Procedure
  - Stay up to date with newly-identified technical vulnerabilities.

    - Stay up to date with new threats, including weather, civil unrest, disaster warnings, that can impact the organization's critical functions and staff.

- CC19.1 - Incident Response Plan: Ensure that an effective Incident Response Plan is in place and managed.

  Procedure
    - Create comprehensive incident response plans that meet all organizational, regulatory, and legal requirements. Require that all incidents be managed.

References

- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- NIST CSF Framework (pdf) - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NIST CSF Framework (Excel) - https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx

Kaseya Cybersecurity Fundamentals CSF Function 5: RC - Recover

Kaseya Cybersecurity Fundamentals	Other Requirements
CSF Function 5: RC Recover	N/A

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

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Guidance
The NIST Cybersecurity Framework's Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Examples of outcome Categories within this Function include:

1. Ensuring the organization implements Recovery Planning processes and procedures to restore systems and/or assets affected by cybersecurity incidents

2. Implementing Improvements based on lessons learned and reviews of existing strategies

3. Internal and external Communications are coordinated during and following the recovery from a cybersecurity incident

Source: NIST Cybersecurity Framework - The Five Functions

https://www.nist.gov/cyberframework/online-learning/five-functions

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

Related Internal Controls
- CC20.1 - Follow Incident Recovery Plan: Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery

  Procedure
  - After an incident, follow your recovery plan rather than an ad-hoc response.

References
- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework

- NIST CSF Framework (pdf) - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NIST CSF Framework (Excel) - https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx