YourIT!
Your Logo Goes Here

# NIST CSF 2.0

## Policies and Procedures

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: Client Company

Prepared by: YourIT Company

# Table of Contents

# Purpose

The purpose is to ensure the security of data aligned with a federal standard, to meet regulatory, contractual, or insurance requirements, or to ensure a high level of data protection.

# Scope

This policy applies to the workforce members and vendors of organization that come in contact with sensitive, confidential, and/or protected data.

# 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.

# NIST CSF 2.0 DE.AE-02 - Potentially Adverse Event Analysis

| **NIST CSF 2.0** | **Other Requirements** |
|---|---|
| DE.AE-02<br>Potentially Adverse Event Analysis | N/A |

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

DE.AE-02: Potentially adverse events are analyzed to better understand associated activities.

**Guidance**
Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Use security information and event management (SIEM) or other tools to continuously monitor log events for known malicious and suspicious activity

Ex2: Utilize up-to-date cyber threat intelligence in log analysis tools to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise

Ex3: Regularly conduct manual reviews of log events for technologies that cannot be sufficiently monitored through automation

Ex4: Use log analysis tools to generate reports on their findings

NIST CSF 2.0 - Informative References:

CIS Controls v8.0: 8.11
CRI Profile v2.0: DE.AE-02
CRI Profile v2.0: DE.AE-02.01
CRI Profile v2.0: DE.AE-02.02
CSF v1.1: DE.AE-2
SP 800-53 Rev 5.1.1: AU-06
SP 800-53 Rev 5.1.1: CA-07
SP 800-53 Rev 5.1.1: IR-04
SP 800-53 Rev 5.1.1: SI-04

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

**Related Internal Controls**

- CIS8.11 - Conduct Audit Log Reviews: Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

**References**

- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- CIS Critical Security Controls - https://www.cisecurity.org/controls
- CRI Profile v2.0 - https://cyberriskinstitute.org/the-profile/
- NIST CSF 1.1 Archive - https://www.nist.gov/cyberframework/csf-11-archive

# NIST CSF 2.0 DE.AE-03 - Event Information Correlation

| **NIST CSF 2.0** | **Other Requirements** |
|---|---|
| DE.AE-03<br>Event Information Correlation | N/A |

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

DE.AE-03: Information is correlated from multiple sources.

**Guidance**
Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Constantly transfer log data generated by other sources to a relatively small number of log servers

Ex2: Use event correlation technology (e.g., SIEM) to collect information captured by multiple sources

Ex3: Utilize cyber threat intelligence to help correlate events among log sources

NIST CSF 2.0 - Informative References:

CRI Profile v2.0: DE.AE-03
CRI Profile v2.0: DE.AE-03.01
CRI Profile v2.0: DE.AE-03.02
CSF v1.1: DE.AE-3
SP 800-53 Rev 5.1.1: AU-06
SP 800-53 Rev 5.1.1: CA-07
SP 800-53 Rev 5.1.1: PM-16
SP 800-53 Rev 5.1.1: IR-04
SP 800-53 Rev 5.1.1: IR-05
SP 800-53 Rev 5.1.1: IR-08
SP 800-53 Rev 5.1.1: SI-04

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

**Related Internal Controls**

- CRI.DE.AE-03.01 - Event Information Correlation.01:
  NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-03.01:

The organization implements systematic and real-time logging, collection, monitoring, detection, and alerting measures across multiple layers of the organization's infrastructure, including physical perimeters, network, operating systems, applications, data, and external (cloud and outsourced) environments, sufficient to protect the organization's information assets.

- CRI.DE.AE-03.02 - Event Information Correlation.02 :
  NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-03.02:

  The organization performs real-time central analysis, aggregation, and correlation of anomalous activities, network and system alerts, and relevant event and cyber threat intelligence, including both internal and external (cloud and outsourced) environments, to better detect and prevent multifaceted cyber attacks.

**References**

- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- CRI Profile v2.0 - https://cyberriskinstitute.org/the-profile/
- NIST CSF 1.1 Archive - https://www.nist.gov/cyberframework/csf-11-archive

# NIST CSF 2.0 DE.AE-04 - Impact & Scope Determination

| | |
|---|---|
| **NIST CSF 2.0**<br>DE.AE-04<br>Impact & Scope Determination | **Other Requirements**<br>N/A |

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

DE.AE-04: The estimated impact and scope of adverse events are understood.

**Guidance**
Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Use SIEMs or other tools to estimate impact and scope, and review and refine the estimates

Ex2: A person creates their own estimates of impact and scope

NIST CSF 2.0 - Informative References:

CRI Profile v2.0: DE.AE-04
CRI Profile v2.0: DE.AE-04.01
CSF v1.1: DE.AE-4
SP 800-53 Rev 5.1.1: PM-09
SP 800-53 Rev 5.1.1: PM-11
SP 800-53 Rev 5.1.1: PM-18
SP 800-53 Rev 5.1.1: PM-28
SP 800-53 Rev 5.1.1: PM-30

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

**Related Internal Controls**

- CRI.DE.AE-04.01 - Impact & Scope Determination:

  NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-04.01:

  The organization has a documented process to analyze and triage incidents to assess root cause, technical impact, mitigation priority, and business impact on the organization, as well as across the financial sector and other third party stakeholders.

**References**

- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- CRI Profile v2.0 - https://cyberriskinstitute.org/the-profile/
- NIST CSF 1.1 Archive - https://www.nist.gov/cyberframework/csf-11-archive

# NIST CSF 2.0 DE.AE-06 - Event Information Sharing

| NIST CSF 2.0 | Other Requirements |
|---|---|
| DE.AE-06<br>Event Information Sharing | N/A |

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

DE.AE-06: Information on adverse events is provided to authorized staff and tools.

**Guidance**
Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Use cybersecurity software to generate alerts and provide them to the security operations center (SOC), incident responders, and incident response tools

Ex2: Incident responders and other authorized personnel can access log analysis findings at all times

Ex3: Automatically create and assign tickets in the organization's ticketing system when certain types of alerts occur

Ex4: Manually create and assign tickets in the organization's ticketing system when technical staff discover indicators of compromise

NIST CSF 2.0 - Informative References:

CRI Profile v2.0: DE.AE-06
CRI Profile v2.0: DE.AE-06.01
CSF v1.1: DE.DP-4
SP 800-53 Rev 5.1.1: IR-04
SP 800-53 Rev 5.1.1: PM-15
SP 800-53 Rev 5.1.1: PM-16
SP 800-53 Rev 5.1.1: RA-04
SP 800-53 Rev 5.1.1: RA-10

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

**Related Internal Controls**

- CRI.DE.AE-06.01 - Event Information Sharing:
  NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-06.01:

  The organization has established processes and protocols to communicate, alert, and regularly report potential cyber attacks and incident information, including its corresponding analysis and cyber threat intelligence, to authorized internal and external stakeholders.

**References**

- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- CRI Profile v2.0 - https://cyberriskinstitute.org/the-profile/
- NIST CSF 1.1 Archive - https://www.nist.gov/cyberframework/csf-11-archive

# NIST CSF 2.0 DE.AE-07 - Contextual Analysis

| **NIST CSF 2.0**<br>DE.AE-07<br>Contextual Analysis | **Other Requirements**<br>N/A |
|---|---|

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

DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis.

**Guidance**
Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Securely provide cyber threat intelligence feeds to detection technologies, processes, and personnel

Ex2: Securely provide information from asset inventories to detection technologies, processes, and personnel

Ex3: Rapidly acquire and analyze vulnerability disclosures for the organization's technologies from suppliers, vendors, and third-party security advisories

NIST CSF 2.0 - Informative References:

CRI Profile v2.0: DE.AE-07
CRI Profile v2.0: DE.AE-07.01
CRI Profile v2.0: DE.AE-07.02
CSF v1.1: DE.AE-3
SP 800-53 Rev 5.1.1: PM-16
SP 800-53 Rev 5.1.1: RA-03
SP 800-53 Rev 5.1.1: RA-10

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

**Related Internal Controls**

- CRI.DE.AE-07.01 - Contextual Analysis.01:
  NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-07.01:

The organization implements measures for monitoring external sources (e.g., social media, the dark web, etc.) to integrate with other intelligence information to better detect and evaluate potential threats and compromises.

- CRI.DE.AE-07.02 - Contextual Analysis.02:
  NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-07.02:

  Relevant event data is packaged for subsequent review and triage and events are categorized for efficient handling, assignment, and escalation.

**References**

- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- CRI Profile v2.0 - https://cyberriskinstitute.org/the-profile/
- NIST CSF 1.1 Archive - https://www.nist.gov/cyberframework/csf-11-archive

# NIST CSF 2.0 DE.AE-08 - Incident Declaration

| | |
|---|---|
| **NIST CSF 2.0**<br>DE.AE-08<br>Incident Declaration | **Other Requirements**<br>N/A |

## Policy

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

DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria.

## Guidance

Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Apply incident criteria to known and assumed characteristics of activity in order to determine whether an incident should be declared

Ex2: Take known false positives into account when applying incident criteria

NIST CSF 2.0 - Informative References:

CRI Profile v2.0: DE.AE-08
CRI Profile v2.0: DE.AE-08.01
CSF v1.1: DE.AE-5
SP 800-53 Rev 5.1.1: IR-04
SP 800-53 Rev 5.1.1: IR-08

## Responsibilities

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

## Related Internal Controls

- CRI.DE.AE-08.01 - Incident Declaration:

  NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-08.01:

  Defined criteria and severity levels are in place to facilitate the declaration, escalation, organization, and alignment of response activities to response plans within the organization and across relevant third parties.

## References

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

- CRI Profile v2.0 - https://cyberriskinstitute.org/the-profile/
- NIST CSF 1.1 Archive - https://www.nist.gov/cyberframework/csf-11-archive

# NIST CSF 2.0 DE.CM-01 - Network Monitoring

| **NIST CSF 2.0** | **Other Requirements** |
|---|---|
| DE.CM-01<br>Network Monitoring | N/A |

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

DE.CM-01: Networks and network services are monitored to find potentially adverse events.

**Guidance**
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Monitor DNS, BGP, and other network services for adverse events

Ex2: Monitor wired and wireless networks for connections from unauthorized endpoints

Ex3: Monitor facilities for unauthorized or rogue wireless networks

Ex4: Compare actual network flows against baselines to detect deviations

Ex5: Monitor network communications to identify changes in security postures for zero trust purposes

NIST CSF 2.0 - Informative References:

CIS Controls v8.0: 13.1
CRI Profile v2.0: DE.CM-01
CRI Profile v2.0: DE.CM-01.01
CRI Profile v2.0: DE.CM-01.02
CRI Profile v2.0: DE.CM-01.03
CRI Profile v2.0: DE.CM-01.04
CRI Profile v2.0: DE.CM-01.05
CRI Profile v2.0: DE.CM-01.06
CSF v1.1: DE.CM-1
CSF v1.1: DE.CM-4
CSF v1.1: DE.CM-5
CSF v1.1: DE.CM-7
SP 800-53 Rev 5.1.1: AC-02
SP 800-53 Rev 5.1.1: AU-12

SP 800-53 Rev 5.1.1: CA-07
SP 800-53 Rev 5.1.1: CM-03
SP 800-53 Rev 5.1.1: SC-05
SP 800-53 Rev 5.1.1: SC-07
SP 800-53 Rev 5.1.1: SI-04

**Responsibilities**

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

**Related Internal Controls**

- CIS13.1 - Centralize Security Event Alerting: Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

**References**

- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- CIS Critical Security Controls - https://www.cisecurity.org/controls
- CRI Profile v2.0 - https://cyberriskinstitute.org/the-profile/
- NIST CSF 1.1 Archive - https://www.nist.gov/cyberframework/csf-11-archive

# NIST CSF 2.0 DE.CM-02 - Physical Environment Monitoring

| **NIST CSF 2.0** | **Other Requirements** |
|---|---|
| DE.CM-02<br>Physical Environment Monitoring | N/A |

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

DE.CM-02: The physical environment is monitored to find potentially adverse events.

**Guidance**
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Monitor logs from physical access control systems (e.g., badge readers) to find unusual access patterns (e.g., deviations from the norm) and failed access attempts

Ex2: Review and monitor physical access records (e.g., from visitor registration, sign-in sheets)

Ex3: Monitor physical access controls (e.g., locks, latches, hinge pins, alarms) for signs of tampering

Ex4: Monitor the physical environment using alarm systems, cameras, and security guards

NIST CSF 2.0 - Informative References:

CRI Profile v2.0: DE.CM-02
CRI Profile v2.0: DE.CM-02.01
CSF v1.1: DE.CM-2
SP 800-53 Rev 5.1.1: CA-07
SP 800-53 Rev 5.1.1: PE-03
SP 800-53 Rev 5.1.1: PE-06
SP 800-53 Rev 5.1.1: PE-20

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

**Related Internal Controls**

- CRI.DE.CM-02.01 - Physical Environment Monitoring:
  NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.CM-02.01:

The organization's controls include monitoring and detection of anomalous activities and potential intrusion events across the organization's physical environment and infrastructure, including the detection of environmental threats (fire, water, service outages, etc.) and unauthorized physical access to high-risk system components and locations.

**References**

- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- CRI Profile v2.0 - https://cyberriskinstitute.org/the-profile/
- NIST CSF 1.1 Archive - https://www.nist.gov/cyberframework/csf-11-archive

# NIST CSF 2.0 DE.CM-03 - Personnel Activity Monitoring

| **NIST CSF 2.0** | **Other Requirements** |
|---|---|
| DE.CM-03<br>Personnel Activity Monitoring | N/A |

### Policy

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

DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events.

### Guidance

Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Use behavior analytics software to detect anomalous user activity to mitigate insider threats

Ex2: Monitor logs from logical access control systems to find unusual access patterns and failed access attempts

Ex3: Continuously monitor deception technology, including user accounts, for any usage

NIST CSF 2.0 - Informative References:

CIS Controls v8.0: 10.7
CRI Profile v2.0: DE.CM-03
CRI Profile v2.0: DE.CM-03.01
CRI Profile v2.0: DE.CM-03.02
CRI Profile v2.0: DE.CM-03.03
CSF v1.1: DE.CM-3
CSF v1.1: DE.CM-7
SP 800-53 Rev 5.1.1: AC-02
SP 800-53 Rev 5.1.1: AU-12
SP 800-53 Rev 5.1.1: AU-13
SP 800-53 Rev 5.1.1: CA-07
SP 800-53 Rev 5.1.1: CM-10
SP 800-53 Rev 5.1.1: CM-11

### Responsibilities

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

**Related Internal Controls**

- CIS10.7 - Use Behavior-Based Anti-Malware Software: Use behavior-based anti-malware software.

**References**

- NIST Cybersecurity Framework - https://www.nist.gov/cyberframework
- CIS Critical Security Controls - https://www.cisecurity.org/controls
- CRI Profile v2.0 - https://cyberriskinstitute.org/the-profile/
- NIST CSF 1.1 Archive - https://www.nist.gov/cyberframework/csf-11-archive

**Truncated Sample Document**