# NIST Cybersecurity Framework

# Policy Template Guide

**Contents**

## Introduction

The Multi-State Information Sharing & Analysis Center (MS-ISAC) is offering this guide to participants of the Nationwide Cybersecurity Review (NCSR) and MS-ISAC members, as a resource to assist with the application and advancement of cybersecurity policies.

The policy templates are provided courtesy of the SANS Institute (https://www.sans.org/), the State of New York, and the State of California. The templates can be customized and used as an outline of an organizational policy, with additional details to be added by the end user.

The NCSR question set represents the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). This guide gives the correlation between 49 of the NIST CSF subcategories, and applicable policy and standard templates. A NIST subcategory is represented by text, such as "ID.AM-5." This represents the NIST function of Identify and the category of Asset Management.

For additional information on services provided by the Multi-State Information Sharing & Analysis Center (MS-ISAC), please refer to the following page: https://www.cisecurity.org/ms-isac/services/. These policy templates are also mapped to the resources MS-ISAC and CIS provide, open source resources, and free FedVTE training: https://www.cisecurity.org/wp-content/uploads/2019/11/Cybersecurity-Resources-Guide.pdf.

**Disclaimer:** These policies may not reference the most recent applicable NIST revision, however may be used as a baseline template for end users.

# Identify

**Identify:** Asset Management (ID.AM)

**ID.AM-1**    **Physical devices and systems within the organization are inventoried.**

↗Acceptable Use of Information Technology Resource Policy
Access Control Policy
Account Management/Access Control Standard
Identification and Authentication Policy
Information Security Policy
Security Assessment and Authorization Policy
Security Awareness and Training Policy

**ID.AM-2**    **Software platforms and applications within the organization are inventoried.**

Acceptable Use of Information Technology Resource Policy
Access Control Policy
Account Management/Access Control Standard
Identification and Authentication Policy
Information Security Policy
Security Assessment and Authorization Policy
Security Awareness and Training Policy

**ID.AM-4**    **External information systems are catalogued.**

System and Communications Protection Policy

**ID.AM-5**    **Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value).**

SANS Policy Template: Acquisition Assessment Policy
Information Classification Standard
Information Security Policy

**ID.AM-6**    **Cybersecurity roles and responsibilities for the entire workforces and third-party stakeholders (e.g. suppliers, customers, partners) are established.**

Acceptable Use of Information Technology Resource Policy
Information Security Policy
Security Awareness and Training Policy

**Identify: Risk Management Strategy (ID.RM)**

      **ID.RM-1**    **Risk management processes are established, managed, and agreed to by organizational stakeholders.**

                  Information Security Policy
                  Information Security Risk Management Standard
                  Risk Assessment Policy

**Identify: Supply Chain Risk Management (ID.SC)**

      **ID.SC-2**    **Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.**

                  SANS Policy Template: Acquisition Assessment Policy
                  Identification and Authentication Policy
                  Security Assessment and Authorization Policy
                  Systems and Services Acquisition Policy

      **ID.SC-4**    **Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.**

                  SANS Policy Template: Acquisition Assessment Policy
                  Identification and Authentication Policy
                  Security Assessment and Authorization Policy
                  Systems and Services Acquisition Policy

      **ID.SC-5**    **Response and recovery planning and testing are conducted with suppliers and third-party providers.**

                  SANS Policy Template: Security Response Plan Policy
                  Computer Security Threat Response Policy
                  Cyber Incident Response Standard
                  Incident Response Policy
                  Systems and Services Acquisition Policy

# Protect

**Protect: Identity Management and Access Control (PR.AC)**

**PR.AC-1** **Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.**

Access Control Policy
Account Management/Access Control Standard
Authentication Tokens Standard
Configuration Management Policy
Identification and Authentication Policy
Sanitization Secure Disposal Standard
Secure Configuration Standard
Secure System Development Life Cycle Standard

**PR.AC-3** **Remote access is managed.**

SANS Policy Template: Remote Access Policy
Remote Access Standard

**PR.AC-4** **Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.**

Access Control Policy
Account Management/Access Control Standard
Authentication Tokens Standard
Configuration Management Policy
Identification and Authentication Policy
Sanitization Secure Disposal Standard
Secure Configuration Standard
Secure System Development Life Cycle Standard

**PR.AC-5** **Network integrity is protected (e.g., network segregation, network segmentation).**

SANS Policy Template: Lab Security Policy
SANS Policy Template: Router and Switch Security Policy
802.11 Wireless Network Security Standard
Mobile Device Security
System and Information Integrity Policy

**Protect: Awareness and Training (PR.AT)**

**PR.AT-1**   **All users are informed and trained.**

Acceptable Use of Information Technology Resources Policy
Information Security Policy
Personnel Security Policy
Physical and Environmental Protection Policy
Security Awareness and Training Policy

**Protect: Data Security (PR.DS)**

**PR.DS-1**   **Data-at-rest is protected**

Computer Security Threat Response Policy
Cyber Incident Response Standard
Encryption Standard
Incident Response Policy
Information Security Policy
Maintenance Policy
Media Protection Policy
Mobile Device Security
Patch Management Standard

**PR.DS-2**   **Data-in-transit is protected.**

Computer Security Threat Response Policy
Cyber Incident Response Standard
Encryption Standard
Incident Response Policy
Information Security Policy
Maintenance Policy
Media Protection Policy
Mobile Device Security
Patch Management Standard

**PR.DS-3**   **Assets are formally managed throughout removal, transfers, and disposition.**

SANS Policy Template: Acquisition Assessment Policy
SANS Policy Template: Technology Equipment Disposal Policy
Access Control Policy
Account Management/Access Control Standard
Authentication Tokens Standard
Configuration Management Policy
Identification and Authentication Policy
Sanitization Secure Disposal Standard
Secure Configuration Standard
Secure System Development Life Cycle Standard

**PR.DS-7**   The development and testing environment(s) are separate from the production environment.

SANS Policy Template: Lab Security Policy
SANS Policy Template: Router and Switch Security Policy

**PR.DS-8**   Integrity checking mechanisms are used to verify hardware integrity.

SANS Policy Template: Acquisition Assessment Policy
System and Information Integrity Policy

**Protect: Information Protection Processes and Procedures (PR.IP)**

**PR.IP-1**   A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).

Access Control Policy
Account Management/Access Control Standard
Authentication Tokens Standard
Configuration Management Policy
Identification and Authentication Policy
Sanitization Secure Disposal Standard
Secure Configuration Standard
Secure System Development Life Cycle Standard

**PR.IP-4**   Backups of information are conducted, maintained, and tested.

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Encryption Standard
Incident Response Policy
Information Security Policy
Maintenance Policy
Media Protection Policy
Mobile Device Security
Patch Management Standard

**PR.IP-6**   Data is destroyed according to policy.

SANS Policy Template: Technology Equipment Disposal Policy
Maintenance Policy
Media Protection Policy
Sanitization Secure Disposal Standard

**PR.IP-9**    Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Disaster Recovery Plan Policy
SANS Policy Template: Pandemic Response Planning
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy
Planning Policy

**PR.IP-10**    Response and recovery plans are tested.

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Disaster Recovery Plan Policy
SANS Policy Template: Pandemic Response Planning
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy
Planning Policy

## Protect: Maintenance (PR.MA)

**PR.MA-2**    Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.

SANS Policy Template: Remote Access Policy
SANS Policy Template: Remote Access Tools Policy
Maintenance Policy
Remote Access Standard
Security Logging Standard

## Protect: Protective Technology (PR.PT)

**PR.PT-1**    Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.

SANS Policy Template: Information Logging Standard
Access Control Policy
Account Management/Access Control Standard
Authentication Tokens Standard
Configuration Management Policy
Identification and Authentication Policy
Sanitization Secure Disposal Standard
Secure Configuration Standard
Secure System Development Life Cycle Standard
Security Logging Standard

**PR.PT-2**    Removable media is protected and its use restricted according to policy.

SANS Policy Template: Acceptable Use Policy
Acceptable Use of Technology Resources Policy
Media Protection Policy
Mobile Device Security

**PR.PT-4**    Communications and control networks are protected.

SANS Policy Template: Router and Switch Security Policy
Encryption Standard
Information Security Policy
Maintenance Policy
Media Protection Policy
Mobile Device Security
System and Communications Protection Policy

**PR.PT-5**    Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

SANS Policy Template: Disaster Recovery Plan Policy
SANS Policy Template: Security Response Plan Policy

# Detect

## Detect: Anomalies and Events (DE.AE)

**DE.AE-3**   **Event data are collected and correlated from multiple sources and sensors.**

SANS Policy Template: Information Logging Standard
Auditing and Accountability Standard
Security Logging Standard
System and Information Integrity Policy
Vulnerability Scanning Standard

## Detect: Security Continuous Monitoring (DE.CM)

**DE.CM-1**   **The network is monitored to detect potential cybersecurity events.**

SANS Policy Template: Router and Switch Security Policy
Encryption Standard
Information Security Policy
Maintenance Policy
Media Protection Policy
Mobile Device Security
Patch Management Standard
Security Assessment and Authorization Policy
Vulnerability Scanning Standard

**DE.CM-4**   **Malicious code is detected.**

Auditing and Accountability Standard
Secure Coding Standard
Security Logging Standard
System and Information Integrity Policy
Vulnerability Scanning Standard

**DE.CM-7**   **Monitoring for unauthorized personnel, connections, devices, and software is performed.**

Auditing and Accountability Standard
Security Logging Standard
System and Information Integrity Policy
Vulnerability Scanning Standard

**DE.DP-1**    **Roles and responsibilities for detection are well defined to ensure accountability.**

Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy
Information Security Policy

**DE.DP-4**    **Event detection information is communicated.**

Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy
Information Security Policy

NIST FUNCTION:

# Respond

## Respond: Response Planning (RS.RP)6

**RS.RP-1**    **Response plan is executed during or after an event.**

SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy
Planning Policy

## Respond: Communications (RS.CO)

**RS.CO-1**    **Personnel know their roles and order of operations when a response is needed.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

**RS.CO-2**    **Incidents are reported consistent with established criteria.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

**RS.CO-3**    **Information is shared consistent with response plans.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

**RS.CO-4**    **Coordination with stakeholders occurs consistent with response plans**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

**RS.CO-5**    **Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

## Respond: Analysis (RS.AN)

**RS.AN-4**    **Incidents are categorized consistent with response plans.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

## Respond: Improvements (RS.IM)

**RS.IM-1**    **Response plans incorporate lessons learned.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

**RS.IM-2**    **Response strategies are updated.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

NIST FUNCTION:

# Recover

## Recover: Recovery Planning (RC.RP)

**RC.RP-1**  **Recovery plan is executed during or after a cybersecurity incident.**

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Contingency Planning Policy
Cyber Incident Response Standard
Incident Response Policy

## Recover: Improvements (RC.IM)

**RC.IM-1**  **Recovery plans incorporate lessons learned.**

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Contingency Planning Policy
Cyber Incident Response Standard
Incident Response Policy

**RC.IM-2**  **Recovery strategies are updated.**

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Contingency Planning Policy
Cyber Incident Response Standard
Incident Response Policy

## Recover: Communications (RC.CO)

**RC.CO-1**  **Public relations are managed.**

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

**RC.CO-2**  **Reputation is repaired after an incident.**

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

**RC.CO-3**   **Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.**

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

# Additional Policy Templates

The following policy templates address additional functions and processes related to an organization's information security:

**General**

Acceptable Encryption Policy
Clean Desk Policy
Digital Signature Acceptance Policy
Email Policy
Ethics Policy
Password Construction Guidelines
Password Protection Policy
Secure Use of Social Media Guideline
Continuing Professional Education Requirements for Information Security Officers/
Designated Security Representatives
Information Security Exception Policy

**Network**

Bluetooth Baseline Requirements Policy
Wireless Communication Policy
Wireless Communication Standard

**Server Security**

Database Credentials Policy Server Security Policy
Software Installation Policy
Workstation Security (For HIPAA) Policy

**Application Security**

Web Application Security Policy