CIS® Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

NIST Cybersecurity Framework

# SANS Policy Templates

## Introduction

The Multi-State Information Sharing & Analysis Center (MS-ISAC) is offering this guide to the SLTT community, 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 templates can be used as an outline of an organizational policy, with additional details to be added by the end user.

The framework referenced in this guide is the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) (https://www.nist.gov/). This guide gives the correlation between 35 of the NIST CSF subcategories, and applicable SANS policy 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/.

# NIST Function:Identify

## Identify – Asset Management (ID.AM)

**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

## 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

**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

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

SANS Policy Template: Security Response Plan Policy

# NIST Function:Protect

## Protect – Identity Management and Access Control (PR.AC)

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

SANS Policy Template: Remote Access Policy

**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

## Protect – Data Security (PR.DS)

**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

**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

## Protect – Information Protection Processes and Procedures (PR.IP)

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

SANS Policy Template: Disaster Recovery Plan Policy

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

SANS Policy Template: Technology Equipment Disposal Policy

**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

**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

## 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

## 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

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

SANS Policy Template: Acceptable Use Policy

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

SANS Policy Template: Router and Switch Security 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

# NIST Function: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**

# NIST Function:Respond

## Respond – Response Planning (RS.RP)

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

SANS Policy Template: Security Response Plan 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

**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

**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

**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

**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

## 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

## 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

**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

# 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

## Recover – Improvements (RC.IM)

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

SANS Policy Template: Disaster Recovery Plan Policy

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

SANS Policy Template: Disaster Recovery Plan Policy

## Recover – Communications (RC.CO)

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

SANS Policy Template: Disaster Recovery Plan Policy

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

SANS Policy Template: Disaster Recovery Plan 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

# Additional SANS 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

## 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