NIST CSF

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

YourIT!
Your Logo Goes Here

Table of Contents

30	NIST CSF PR.AC-3 - Remote access
31	NIST CSF PR.AC-4 - Access permissions
32	NIST CSF PR.AC-5 - Network integrity
33	NIST CSF PR.AT-1 - Training
34	NIST CSF PR.AT-2 - Privileged users
35	NIST CSF PR.AT-3 - Third-party stakeholders
36	NIST CSF PR.AT-4 - Senior executives
37	NIST CSF PR.AT-5 - Physical and information security personnel
38	NIST CSF PR.DS-1 - Data-at-rest
39	NIST CSF PR.DS-2 - Data-in-transit
40	NIST CSF PR.DS-3 - Asset management
41	NIST CSF PR.DS-4 - Capacity
42	NIST CSF PR.DS-5 - Data leak protection
43	NIST CSF PR.DS-6 - Integrity checking
44	NIST CSF PR.DS-7 - Development & testing environments
45	NIST CSF PR.IP-1 - Baseline configurations
46	NIST CSF PR.IP-2 - System Development Life Cycle
47	NIST CSF PR.IP-3 - Configuration change control
48	NIST CSF PR.IP-4 - Backups
49	NIST CSF PR.IP-5 - Physical operating environment
50	NIST CSF PR.IP-6 - Data destruction
51	NIST CSF PR.IP-7 - Continuous improvement
52	NIST CSF PR.IP-8 - Sharing information
53	NIST CSF PR.IP-9 - Incident Response and Business Continuity Plans
54	NIST CSF PR.IP-10 - Incident response and recovery plan testing
55	NIST CSF PR.IP-11 - Human Resource practices
56	NIST CSF PR.IP-12 - Vulnerability management
57	NIST CSF PR.MA-1 - Maintenance
58	NIST CSF PR.MA-2 - Remote maintenance
59	NIST CSF PR.PT-1 - Logging & Audit Controls
60	NIST CSF PR.PT-2 - Removable media
61	NIST CSF PR.PT-3 - Least functionality

62	NIST CSF PR.PT-4 - Communications protection
63	NIST CSF DE.AE-1 - Network operations baseline
64	NIST CSF DE.AE-2 - Analyze events
65	NIST CSF DE.AE-3 - Data aggregation and correlation
66	NIST CSF DE.AE-4 - Event impact
67	NIST CSF DE.AE-5 - Incident alerts
68	NIST CSF DE.CM-1 - Network monitoring
69	NIST CSF DE.CM-2 - Physical environment monitoring
70	NIST CSF DE.CM-3 - Personnel monitoring
71	NIST CSF DE.CM-4 - Malicious code detection
72	NIST CSF DE.CM-5 - Mobile code
73	NIST CSF DE.CM-6 - External service provider monitoring
74	NIST CSF DE.CM-7 - Unauthorized activity monitoring
75	NIST CSF DE.CM-8 - Vulnerability scans
76	NIST CSF DE.DP-1 - Detection roles and responsibilities
77	NIST CSF DE.DP-2 - Detection compliance
78	NIST CSF DE.DP-3 - Test detection processes
79	NIST CSF DE.DP-4 - Communicate detections
80	NIST CSF DE.DP-5 - Detection continuous improvement
81	NIST CSF RS.RP-1 - Execute response plans
82	NIST CSF RS.CO-1 - Response roles and responsibilities.
83	NIST CSF RS.CO-2 - Event reporting
84	NIST CSF RS.CO-3 - Response information sharing
85	NIST CSF RS.CO-4 - Response coordination
86	NIST CSF RS.CO-5 - Voluntary information sharing
87	NIST CSF RS.AN-1 - Investigate notifications
88	NIST CSF RS.AN-2 - Incident impact
89	NIST CSF RS.AN-3 - Perform forensics
90	NIST CSF RS.AN-4 - Categorize incidents
91	NIST CSF RS.MI-1 - Contain incidents
92	NIST CSF RS.MI-2 - Mitigate incidents
93	NIST CSF RS.MI-3 - Newly identified vulnerabilities

94	NIST CSF RS.IM-1 - Response lessons learned
95	NIST CSF RS.IM-2 - Update response strategies
96	NIST CSF RC.RP-1 - Execute recovery plan
97	NIST CSF RC.IM-1 - Recovery lessons learned
98	NIST CSF RC.IM-2 - Update recovery strategies
99	NIST CSF RC.CO-1 - Manage public relations
100	NIST CSF RC.CO-2 - Reputation repair
101	NIST CSF RC.CO-3 - Communicate recovery activities
102	NIST CSF RS.AN-5 - Vulnerability processes
103	NIST CSF ID.SC-1 - Supply Chain Risk Management
104	NIST CSF ID.SC-2 - Supply Chain Risk Assessment
105	NIST CSF ID.SC-3 - Supply Chain Contracts
106	NIST CSF ID.SC-4 - Supply Chain Evaluations
107	NIST CSF ID.SC-5 - Supply Chain Response and Recovery
108	NIST CSF PR.PT-5 - Resilience Mechanisms
109	NIST CSF PR.DS-8 - Hardware Integrity
110	NIST CSF PR.AC-6 - Identity Proof
111	NIST CSF PR.AC-7 - Authentication

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 ID.AM-1 - Hardware inventory

NIST CSF	Other Requirements
ID.AM-1 Hardware inventory	N/A

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

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

Guidance
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

This requirement includes all devices and systems that access data, including computers, laptops, mobile devices (smartphones and tablets), removable media, portable media, and cloud services.

While a network scan will identify network devices, everything else will need to be manually inventoried.

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, hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware) throughout the respective system development life cycles.

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

NIST CSF ID.AM-2 - Software and Platform Inventory

NIST CSF	Other Requirements
ID.AM-2 Software and Platform Inventory	N/A

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

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

Guidance
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

This requirement includes all software that accesses, processes, or stores data, including on computers, laptops, mobile devices (smartphones and tablets), removable media, portable media, and cloud services.

While a network scan will identify software programs, everything else will need to be manually inventoried.

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, hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware) throughout the respective system development life cycles.

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

NIST CSF ID.AM-3 - Data Flows

NIST CSF	Other Requirements
ID.AM-3 Data Flows	N/A

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

ID.AM-3: Organizational communication and data flows are mapped

Guidance
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

This cannot be automated. Data flows need to be diagramed and documented, and updated as changes occur.

It requires the involvement of department heads and organizational subject matter experts who understand and can describe how data flows within, and in and out of, the organization.

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, hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware) throughout the respective system development life cycles.
- CC1.2 - Data Locations: Locate and identify all organizational data, including data stored on local devices, mobile devices, servers, mass storage, portable media, and cloud platforms.
- CC1.3 - Data Flow Mapping: Create a map of how data flows within and in/out of the organization.

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

NIST CSF ID.AM-4 - External Information Systems

NIST CSF	Other Requirements
ID.AM-4 External Information Systems	N/A

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

ID.AM-4: External information systems are catalogued

Guidance
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

Cloud services and other organizations' systems that are accessed remotely must be documented. This includes portals used to share information.

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, hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware) throughout the respective system development life cycles.

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

NIST CSF ID.AM-5 - Resource and Data Prioritization

NIST CSF	Other Requirements
ID.AM-5 Resource and Data Prioritization	N/A

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

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

Guidance
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

All resources and data should be prioritized to support contingency planning.

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

Related Internal Controls
- CC14.2 - Resource Criticality: Establish and communicate the criticality of all resources.

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

NIST CSF ID.AM-6 - Cybersecurity Roles and Responsibilities

NIST CSF	Other Requirements
ID.AM-6 Cybersecurity Roles and Responsibilities	N/A

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

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

Guidance
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

Cybersecurity roles and responsibilities must be assigned to qualified staff and outsourced vendors. This requires written job descriptions, cybersecurity plans, and procedures.

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

Related Internal Controls
- CC2.4 - Workforce Cybersecurity Roles & Responsibilities: Establish and document cybersecurity roles and responsibilities within the workforce.

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

NIST CSF ID.BE-1 - Supply Chain Role

NIST CSF	Other Requirements
ID.BE-1 Supply Chain Role	N/A

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

ID.BE-1: The organization's role in the supply chain is identified and communicated

Guidance
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

By understanding the organization's role in the supply chain, it can better plan its operations and contingency requirements.

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

Related Internal Controls
- CC2.1 - Organization's Supply Chain Role: Identify and communicate the organization's role in the supply chain.

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

NIST CSF ID.BE-2 - Critical Infrastructure Role

NIST CSF	Other Requirements
ID.BE-2 Critical Infrastructure Role	N/A

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

ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated

Guidance
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

By identifying its role in critical infrastructure, the organization can better understand what regulations, requirements, and resources it will need.

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

Related Internal Controls
- CC2.2 - Organization's Critical Infrastructure Role: Identify and communicate the organization's role in critical infrastructure.

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

NIST CSF ID.BE-3 - Priorities

NIST CSF	Other Requirements
ID.BE-3 Priorities	N/A

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

ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated

Guidance
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

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

Related Internal Controls
- CC14.4 - Organizational Priorities: Establish and communicate priorities based on the organization's mission, objectives, activities, legal requirements, and regulations.

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

NIST CSF ID.BE-4 - Dependencies

NIST CSF	Other Requirements
ID.BE-4 Dependencies	N/A

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

ID.BE-4: Dependencies and critical functions for delivery of critical services are established

Guidance
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

This is one of the most critical requirements for a successful Business Continuity Plan.

Accurately identifying dependencies is critical to contingency planning. If a dependency is missed, it may cause a critical function to fail.

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

Related Internal Controls
- CC14.7 - Dependencies: Identify and document all dependencies for each critical function. Include technology, people, and facilities.

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

NIST CSF ID.BE-5 - Resilience

NIST CSF	Other Requirements
ID.BE-5 Resilience	N/A

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

ID.BE-5: Resilience requirements to support delivery of critical services are established

Guidance
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

Resilience includes backups, alternate equipment, restoration sites, cross-trained personnel, redundant power and communications, and insurance.

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

Related Internal Controls
- CC14.8 - Resiliency Requirements: Establish resilience requirements to support the delivery of critical services.

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

NIST CSF ID.GV-1 - Security Policy

NIST CSF	Other Requirements
ID.GV-1 Security Policy	N/A

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

ID.GV-1: Organizational information security policy is established.

Guidance
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

Organizational cybersecurity policies are the foundation for determining procedures and what evidence of compliance will be required.

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

Related Internal Controls
- CC4.1 - Written Cybersecurity Policies: Write policies addressing all cybersecurity requirements.

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

NIST CSF ID.GV-2 - Coordination

NIST CSF	Other Requirements
ID.GV-2 Coordination	N/A

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

ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners

Guidance
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

Because the dependence on technology is so high in most organizations, it is important to ensure that cybersecurity staff and resources are tied to other departments and clients, vendors, and partners.

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

Related Internal Controls
- CC2.8 - Roles & Responsibilities Coordination: Coordinate and align information security roles & responsibilities with internal roles and external partners.

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

Truncated Sample Report