#	NIST Cybersecurity Framework Policy	Policy Description
1	**Asset Management** NIST Cybersecurity Framework Reference NIST CsF: Asset Management (ID.AM)	To describe the activities required to perform Asset Management (e.g., identify and manage business purposes).
2	**Physical Devices Inventory Policy** NIST Cybersecurity Framework Reference NIST CsF: Asset Management Physical Devices Inventory (ID.AM-1)	To describe the activities required to perform an inventory of the organization's physical assets and systems.
3	**Software and Application Inventory Policy** NIST Cybersecurity Framework Reference NIST CsF: Asset Management Software and Application Inventory (ID.AM-2)	To describe the activities required to perform an inventory of the organization's software and applications.
4	**Communication and Data Flow Policy** NIST Cybersecurity Framework Reference NIST CsF: Asset Management Communication and Data Flow (ID.AM-3)	To map data flows and organizational communication.
5	**External Information System Catalog Policy** NIST Cybersecurity Framework Reference NIST CsF: Asset Management External Information System Catalog (ID.AM-4)	To catalog external information systems.
6	**Resource Priority Policy** NIST Cybersecurity Framework Reference NIST CsF: Asset Management Resource Priority (ID.AM-5)	To classify and prioritize the organization's resources.
7	**Workforce and Stakeholders Roles and Responsibilities Policy** NIST Cybersecurity Framework Reference NIST CsF: Asset Management Workforce and Stakeholders Roles and Responsibilities (ID.AM-6)	To establish roles and responsibilities for workforce and stakeholders.
8	**Business Environment** NIST Cybersecurity Framework Reference NIST CsF: Business Environment (ID.BE)	To describe the organizational cybersecurity roles and risk management decisions.

#	NIST Cybersecurity Framework Policy	Policy Description
9	**Supply Chain Policy** NIST Cybersecurity Framework Reference NIST CsF: Business Environment Supply Chain (ID.BE-1)	To identify roles and responsibilities for the supply chain.
10	**Critical Infrastructure Communication Policy** NIST Cybersecurity Framework Reference NIST CsF: Business Environment Critical Infrastructure Communication (ID.BE-2)	To identify critical infrastructure.
11	**Organizational Mission, Objectives, and Activities Policy** NIST Cybersecurity Framework Reference NIST CsF: Business Environment Organizational Mission, Objectives and Activities (ID.BE-3)	To establish the organization's mission, objective and activities.
12	**Critical Services Delivery Policy** NIST Cybersecurity Framework Reference NIST CsF: Business Environment Critical Services Delivery (ID.BE-4)	To establish critical functions for critical services.
13	**Critical Services Delivery Support Policy** NIST Cybersecurity Framework Reference NIST CsF: Business Environment Critical Services Delivery Support (ID.BE-5)	To establish recovery requirements for critical services.
14	**Governance** NIST Cybersecurity Framework Reference NIST CsF: Governance (ID.GV)	To establish organizational policies, processes and procedures for information security and risk management.
15	**Cybersecurity Policy** NIST Cybersecurity Framework Reference NIST CsF: Governance Cybersecurity Policy (ID.GV-1)	To create and communicate the cybersecurity program.

#	NIST Cybersecurity Framework Policy	Policy Description
16	**External Partners Cybersecurity Roles and Responsibilities Policy** NIST Cybersecurity Framework Reference NIST CsF: Governance External Partners Cybersecurity Roles and Responsibilities (ID.GV-2)	To coordinate roles and responsibilities with third-party personnel.
17	**Cybersecurity Legal and Regulatory Requirements Policy** NIST Cybersecurity Framework Reference NIST CsF: Governance Cybersecurity Legal and Regulatory Requirements (ID.GV-3)	To manage legal and regulatory cybersecurity requirements.
18	**Governance and Risk Management Policy** NIST Cybersecurity Framework Reference NIST CsF: Governance Governance and Risk Management (ID.GV-4)	To create a governance and risk management process.
19	**Risk Assessment** NIST Cybersecurity Framework Reference NIST CsF: Risk Assessment (ID.RA)	To identify the organizational asset vulnerabilities and cybersecurity risk to operations.
20	**Asset Vulnerabilities Policy** NIST Cybersecurity Framework Reference NIST CsF: Risk Assessment Asset Vulnerabilities (ID.RA-1)	To identify asset vulnerabilities.
21	**Cyber Threat Intelligence Policy** NIST Cybersecurity Framework Reference NIST CsF: Risk Assessment Cyber Threat Intelligence (ID.RA-2)	To share threat intelligence.
22	**External and Internal Threats Policy** NIST Cybersecurity Framework Reference NIST CsF: Risk Assessment External and Internal Threats (ID.RA-3)	To identify and document external and internal threats.

#	NIST Cybersecurity Framework Policy	Policy Description
23	**Potential Business Impacts Policy** NIST Cybersecurity Framework Reference NIST CsF: Risk Assessment Potential Business Impacts (ID.RA-4)	To identify potential business impacts.
24	**Determining Risk Policy** NIST Cybersecurity Framework Reference NIST CsF: Risk Assessment Determining Risk (ID.RA-5)	To determine risk for threats and vulnerabilities.
25	**Prioritize Risk Responses Policy** NIST Cybersecurity Framework Reference NIST CsF: Risk Assessment Prioritize Risk Responses (ID.RA-6)	To prioritize risk responses.
26	**Risk Management Strategy** NIST Cybersecurity Framework Reference NIST CsF: Risk Management Strategy (ID.RM)	To describe organizational risk tolerance and established operational risk decisions.
27	**Risk Management Process Policy** NIST Cybersecurity Framework Reference NIST CsF: Risk Management Strategy Risk Management Process (ID.RM-1)	To establish the risk management process by stakeholders.
28	**Determine Risk Tolerance Policy** NIST Cybersecurity Framework Reference NIST CsF: Risk Management Strategy Determine Risk Tolerance (ID.RM-2)	To determine risk tolerance.
29	**Risk Tolerance Policy** NIST Cybersecurity Framework Reference NIST CsF: Risk Management Strategy Risk Tolerance (ID.RM-3)	To determine risk tolerance.
30	**Supply Chain Risk Management** NIST Cybersecurity Framework Reference NIST CsF: Supply Chain Risk Management (ID.SC)	To identify the process for supply chain risk management and to implement contract with suppliers and third-party partners.

#	NIST Cybersecurity Framework Policy	Policy Description
31	**Supply Chain Risk Management Processes Policy** NIST Cybersecurity Framework Reference NIST CsF: Supply Chain Risk Management Supply Chain Risk Management Processes (ID.SC-1)	To identify cyber supply chain risk management processes.
32	**Third Party Services Policy** NIST Cybersecurity Framework Reference NIST CsF: Supply Chain Risk Management Third Party Services (ID.SC-2)	To identify information systems, components and services of third parties.
33	**Cyber Supply Chain Risk Management Plan Policy** NIST Cybersecurity Framework Reference NIST CsF: Supply Chain Risk Management Cyber Supply Chain Risk Management Plan (ID.SC-3)	To ensure contracts with suppliers meet the organization's cybersecurity program objective.
34	**Audit Third Party Partners Policy** NIST Cybersecurity Framework Reference NIST CsF: Supply Chain Risk Management Audit Third Party Partners (ID.SC-4)	To conduct audits on third-party partners.
35	**Response and Recovery Plan Testing Policy** NIST Cybersecurity Framework Reference NIST CsF: Supply Chain Risk Management Response and Recovery Plan Testing (ID.SC-5)	To conduct response and recovery planning and testing with third-party providers.
36	**Management, Authentication and Access Control** NIST Cybersecurity Framework Reference NIST CsF: Management, Authentication and Access Control (PR.AC)	To provide management for limited access to facilities and organization assets.
37	**Identity Management Policy** NIST Cybersecurity Framework Reference NIST CsF: Management, Authentication and Access Control Identity Management (PR.AC-1)	To manage credentials for authorized devices and users.

#	NIST Cybersecurity Framework Policy	Policy Description
38	**Access Management for Assets Policy** NIST Cybersecurity Framework Reference NIST CsF: Management, Authentication and Access Control Access Management for Assets (PR.AC-2)	To protect access to physical assets.
39	**Remote Access Management Policy** NIST Cybersecurity Framework Reference NIST CsF: Management, Authentication and Access Control Remote Access Management (PR.AC-3)	To manage remote access.
40	**Access Authorization Policy** NIST Cybersecurity Framework Reference NIST CsF: Management, Authentication and Access Control Access Authorization (PR.AC-4)	To manage access permissions and authorization.
41	**Network Integrity Policy** NIST Cybersecurity Framework Reference NIST CsF: Management, Authentication and Access Control Network Integrity (PR.AC-5)	To ensure the protection of network integrity.
42	**Proofed Identities Policy** NIST Cybersecurity Framework Reference NIST CsF: Management, Authentication and Access Control Proofed Identities (PR.AC-6)	To ensure identities are proofed and bound to credentials and asserted in interactions.
43	**Authentication Policy** NIST Cybersecurity Framework Reference NIST CsF: Management, Authentication and Access Control Authentication (PR.AC-7)	To ensure authentication of devices and assets.
44	**Awareness and Training** NIST Cybersecurity Framework Reference NIST CsF: Awareness and Training (PR.AT)	To provide cyber security awareness and training to organizational personnel covering their jobs and responsibilities.

#	NIST Cybersecurity Framework Policy	Policy Description
45	**User Training Policy** NIST Cybersecurity Framework Reference NIST CsF: Awareness and Training User Training (PR.AT-1)	To ensure users are trained.
46	**Privileged Users Policy** NIST Cybersecurity Framework Reference NIST CsF: Awareness and Training Privileged Users (PR.AT-2)	To define roles and responsibilities of privileged users.
47	**Third Party Stakeholders Policy** NIST Cybersecurity Framework Reference NIST CsF: Awareness and Training Third-Party Stakeholders (PR.AT-3)	To define roles and responsibilities for third-party stakeholders.
48	**Senior Executives Responsibilities Policy** NIST Cybersecurity Framework Reference NIST CsF: Awareness and Training Senior Executives Responsibilities (PR.AT-4)	To define roles and responsibilities for senior executives.
49	**Cybersecurity Personnel's Responsibilities Policy** NIST Cybersecurity Framework Reference NIST CsF: Awareness and Training Cybersecurity Personnel's Responsibilities (PR.AT-5)	To define roles and responsibilities for cybersecurity personnel.
50	**Data Security** NIST Cybersecurity Framework Reference NIST CsF: Data Security (PR.DS)	To provide risk strategy to ensure the confidentiality, integrity, and availability (CIA) of information assets.
51	**Data at Rest Policy** NIST Cybersecurity Framework Reference NIST CsF: Data Security Data at Rest (PR.DS-1)	To protect data-at-rest.
52	**Data in Transit Policy** NIST Cybersecurity Framework Reference NIST CsF: Data Security Data in Transit (PR.DS-2)	To protect data-in-transit.

#	NIST Cybersecurity Framework Policy	Policy Description
53	**Asset Management and Disposition Policy** NIST Cybersecurity Framework Reference NIST CsF: Data Security Asset Management and Disposition (PR.DS-3)	To manage assets throughout removal, transfers and disposition.
54	**Availability Policy** NIST Cybersecurity Framework Reference NIST CsF: Data Security Availability (PR.DS-4)	To ensure availability.
55	**Data Leaks Protection Policy** NIST Cybersecurity Framework Reference NIST CsF: Data Security Data Leaks Protection (PR.DS-5)	To protect data from leakage.
56	**Integrity Checking Mechanisms Policy** NIST Cybersecurity Framework Reference NIST CsF: Data Security Integrity Checking Mechanisms (PR.DS-6)	Integrity checking mechanisms are used to verify software, firmware and information integrity.
57	**Segregation in Development and Testing Environment(s) Policy** NIST Cybersecurity Framework Reference NIST CsF: Data Security Segregation in Development and Testing Environment(s) (PR.DS-7)	To ensure separation of the testing and production environment.
58	**Hardware Integrity Policy** NIST Cybersecurity Framework Reference NIST CsF: Data Security (PR.DS) Hardware Integrity (PR.DS-8)	To implement integrity mechanisms for hardware.
59	**Information Protection Processes and Procedures** NIST Cybersecurity Framework Reference NIST CsF: Information Protection Processes and Procedures (PR.IP)	To maintain policies, processes and procedures to manage protection of information systems and assets.

#	NIST Cybersecurity Framework Policy	Policy Description
60	**Baseline Configuration Policy** NIST Cybersecurity Framework Reference NIST CsF: Information Protection Processes and Procedures Baseline Configuration (PR.IP-1)	To create a baseline configuration of information technology/industrial control systems.
61	**System Development Life Cycle Policy** NIST Cybersecurity Framework Reference NIST CsF: Information Protection Processes and Procedures System Development Life Cycle (PR.IP-2)	To implement a system development life cycle.
62	**Configuration Change Control Policy** NIST Cybersecurity Framework Reference NIST CsF: Information Protection Processes and Procedures Configuration Change Control (PR.IP-3)	To implement configuration change control processes.
63	**Backup Management Policy** NIST Cybersecurity Framework Reference NIST CsF: Information Protection Processes and Procedures Backup Management (PR.IP-4)	To ensure maintenance and testing of backups.
64	**Physical Operating Environment Policy** NIST Cybersecurity Framework Reference NIST CsF: Information Protection Processes and Procedures Physical Operating Environment (PR.IP-5)	To ensure policy and procedures for the physical operating environment are in place.
65	**Disposal Policy** NIST Cybersecurity Framework Reference NIST CsF: Information Protection Processes and Procedures Disposal (PR.IP-6)	To ensure the disposal of data and assets.
66	**Protection Improvement Policy** NIST Cybersecurity Framework Reference NIST CsF: Information Protection Processes and Procedures Protection Improvement (PR.IP-7)	To improve the protection process.

#	NIST Cybersecurity Framework Policy	Policy Description
67	**Protection Technologies Policy** NIST Cybersecurity Framework Reference NIST CsF: Information Protection Processes and Procedures Protection Technologies (PR.IP-8)	To share effective protection technologies.
68	**Response Plans Availability Policy** NIST Cybersecurity Framework Reference NIST CsF: Information Protection Processes and Procedures Response Plans Availability (PR.IP-9)	To ensure response and recovery plans are in place.
69	**Testing of Response and Recovery Plans Policy** NIST Cybersecurity Framework Reference NIST CsF: Information Protection Processes and Procedures Testing of Response and Recovery Plans (PR.IP-10)	To regularly perform testing of response and recovery plans.
70	**Cybersecurity and Human Resources Policy** NIST Cybersecurity Framework Reference NIST CsF: Information Protection Processes and Procedures Cybersecurity and Human Resources (PR.IP-11)	To ensure cybersecurity is included in human resource practices.
71	**Vulnerability Management Policy** NIST Cybersecurity Framework Reference NIST CsF: Information Protection Processes and Procedures Vulnerability Management (PR.IP-12)	To implement a vulnerability management tool.
72	**Maintenance** NIST Cybersecurity Framework Reference NIST CsF: Maintenance (PR.MA)	To maintain policies and procedures for the maintenance and repairs of organizational assets.
73	**Asset Maintenance and Repair Policy** NIST Cybersecurity Framework Reference NIST CsF: Maintenance Asset Maintenance and Repair (PR.MA-1)	To perform maintenance of assets with controlled tools.

#	NIST Cybersecurity Framework Policy	Policy Description
74	**Remote Maintenance Policy** NIST Cybersecurity Framework Reference NIST CsF: Maintenance Remote Maintenance (PR.MA-2)	To ensure remote maintenance of organizational assets.
75	**Protective Technology** NIST Cybersecurity Framework Reference NIST CsF: Protective Technology (PR.PT)	To provide technical security solutions to ensure the security and protection of systems and organizational assets.
76	**Audit Records Management Policy** NIST Cybersecurity Framework Reference NIST CsF: Protective Technology Audit Records Management (PR.PT-1)	To manage audit records.
77	**Removable Media Protection Policy** NIST Cybersecurity Framework Reference NIST CsF: Protective Technology Removable Media Protection (PR.PT-2)	To protect removable media.
78	**Configuring Essential Capabilities Policy** NIST Cybersecurity Framework Reference NIST CsF: Protective Technology Configuring Essential Capabilities (PR.PT-3)	To provide limited capabilities.
79	**Network Protection Policy** NIST Cybersecurity Framework Reference NIST CsF: Protective Technology Network Protection (PR.PT-4)	To protect communication and control networks.
80	**Mechanism to Achieve Resilience Requirements Policy** NIST Cybersecurity Framework Reference NIST CsF: Protective Technology Mechanism to Achieve Resilience Requirements (PR.PT-5)	To implement mechanisms to manage in normal and adverse situations.
81	**Anomalies and Events** NIST Cybersecurity Framework Reference NIST CsF: Anomalies and Events (DE.AE)	To ensure detection of anomalous activities and events in a timely manner.

#	NIST Cybersecurity Framework Policy	Policy Description
82	**Network Operations Baseline Policy** NIST Cybersecurity Framework Reference NIST CsF: Anomalies and Events Network Operations Baseline (DE.AE-1)	To establish a baseline for network operations and data flows.
83	**Event Detection and Analysis Policy** NIST Cybersecurity Framework Reference NIST CsF: Anomalies and Events Event Detection and Analysis (DE.AE-2)	To analyze events to identify target attacks and methods.
84	**Event Data Collection Policy** NIST Cybersecurity Framework Reference NIST CsF: Anomalies and Events Event Data collection (DE.AE-3)	To collect event data from multiple sources.
85	**Event's Impact Policy** NIST Cybersecurity Framework Reference NIST CsF: Anomalies and Events Event's Impact (DE.AE-4)	To determine the impact of events.
86	**Incident Notification Policy** NIST Cybersecurity Framework Reference NIST CsF: Anomalies and Events Incident Notification (DE.AE-5)	To establish alert notification for incidents.
87	**Security Continuous Monitoring** NIST Cybersecurity Framework Reference NIST CsF: Security Continuous Monitoring (DE.CM)	To ensure monitoring of the physical environment and information system and assets at discrete intervals to identify cybersecurity events.
88	**Network Monitoring Policy** NIST Cybersecurity Framework Reference NIST CsF: Security Continuous Monitoring Network Monitoring (DE.CM-1)	To monitor networks to detect events.
89	**Physical Environment Monitoring Policy** NIST Cybersecurity Framework Reference NIST CsF: Security Continuous Monitoring Physical Environment Monitoring (DE.CM-2)	To monitor the physical environment.

#	NIST Cybersecurity Framework Policy	Policy Description
90	**Personnel Activity Monitoring Policy** NIST Cybersecurity Framework Reference NIST CsF: Security Continuous Monitoring Personnel Activity Monitoring (DE.CM-3)	To monitor personnel activity.
91	**Malicious Code Detection Policy** NIST Cybersecurity Framework Reference NIST CsF: Security Continuous Monitoring Malicious Code Detection (DE.CM-4)	To detect malicious code.
92	**Unauthorized Mobile Code Detection Policy** NIST Cybersecurity Framework Reference NIST CsF: Security Continuous Monitoring Unauthorized Mobile Code Detection (DE.CM-5)	To detect mobile code.
93	**External Service Provider Activity Monitoring Policy** NIST Cybersecurity Framework Reference NIST CsF: Security Continuous Monitoring External Service Provider Activity Monitoring (DE.CM-6)	To monitor external service providers.
94	**Software and Device Monitoring Policy (NIST** NIST Cybersecurity Framework Reference NIST CsF: Security Continuous Monitoring Software and Device Monitoring (DE.CM-7)	To monitor unauthorized assets and personnel.
95	**Vulnerability Scans Policy** NIST Cybersecurity Framework Reference NIST CsF: Security Continuous Monitoring Vulnerability Scans (DE.CM-8)	To perform vulnerability scans.
96	**Detection Processes** NIST Cybersecurity Framework Reference NIST CsF: Detection Processes (DE.DP)	To provide awareness on anomalous events and test detection activities.

#	NIST Cybersecurity Framework Policy	Policy Description
97	**Event Detection Roles and Responsibilities Policy** NIST Cybersecurity Framework Reference NIST CsF: Detection Processes Event detection roles and responsibilities (DE.DP-1)	To define roles and responsibilities for event detection.
98	**Detection Activities Policy** NIST Cybersecurity Framework Reference NIST CsF: Detection Processes Detection Activities (DE.DP-2)	To ensure compliance of detection activities with requirements.
99	**Detection Process Test Policy** NIST Cybersecurity Framework Reference NIST CsF: Detection Processes Detection Process Test (DE.DP-3)	To ensure testing of the detection process.
100	**Event Communication Policy** NIST Cybersecurity Framework Reference NIST CsF: Detection Processes Event Communication (DE.DP-4)	To establish communication of event detection information.
101	**Detection Process Improvement Policy** NIST Cybersecurity Framework Reference NIST CsF: Supply Chain Risk Management Detection Process Improvement (DE.DP-5)	To improve the detection process.
102	**Response Planning** NIST Cybersecurity Framework Reference NIST CsF: Response Planning (RS.RP)	To maintain a response plan to ensure timely response to detected cybersecurity events.
103	**Execute Response Plan Policy** NIST Cybersecurity Framework Reference NIST CsF: Response Planning Execute Response Plan (RS.RP-1)	To maintain a response plan to ensure timely response to detected cybersecurity events.

#	NIST Cybersecurity Framework Policy	Policy Description
104	**Communications (Respond)** NIST Cybersecurity Framework Reference NIST CsF: Communications (Respond) (RS.CO)	To coordinate response activities with stakeholders consistently to achieve broader cybersecurity situational awareness.
105	**Response Roles and Responsibilities Policy** NIST Cybersecurity Framework Reference NIST CsF: Communications (Respond) Response Roles and Responsibilities (RS.CO-1)	To ensure personnel are aware of their roles and responsibilities in regard to incident response.
106	**Reporting Incident Policy** NIST Cybersecurity Framework Reference NIST CsF: Communications (Respond) Reporting Incident (RS.CO-2)	To report incidents per criteria.
107	**Response Plan Policy** NIST Cybersecurity Framework Reference NIST CsF: Communications (Respond) Response Plan (RS.CO-3)	To share information as per response plans.
108	**Response Plan Policy** NIST Cybersecurity Framework Reference NIST CsF: Communications (Respond) Response Plan (RS.CO-4)	To coordinate with stakeholders per response plan.
109	**Cybersecurity Awareness for Stakeholders Policy** NIST Cybersecurity Framework Reference NIST CsF: Supply Chain Risk Management Cybersecurity Awareness for Stakeholders (RS.CO-5)	To create awareness for cybersecurity to stakeholders by sharing voluntary information.
110	**Analysis** NIST Cybersecurity Framework Reference NIST CsF: Analysis (RS.AN)	To conduct analysis to understand response and recovery activities.
111	**Notification Investigation Policy** NIST Cybersecurity Framework Reference NIST CsF: Analysis Notification Investigation (RS.AN-1)	To investigate notifications from detection systems.

#	NIST Cybersecurity Framework Policy	Policy Description
112	**Understanding incident Impact Policy** NIST Cybersecurity Framework Reference NIST CsF: Analysis Understanding Incident Impact (RS.AN-2)	To identify the impact of incidents.
113	**Incident Forensics Policy** NIST Cybersecurity Framework Reference NIST CsF: Analysis Incident Forensics (RS.AN-3)	To ensure forensics is performed after an incident.
114	**Incidents Categorization Policy** NIST Cybersecurity Framework Reference NIST CsF: Analysis (RS.AN) Incidents Categorization (RS.AN-4)	To categorize incidents.
115	**Internal and External Vulnerability Policy** NIST Cybersecurity Framework Reference NIST CsF: Analysis Internal and External Vulnerability (RS.AN-5)	To establish process to receive and respond to vulnerabilities from external or internal sources.
116	**Mitigation** NIST Cybersecurity Framework Reference NIST CsF: Mitigation (RS.MI)	To perform activities to mitigate incident and newly identified vulnerabilities.
117	**Contained Incidents Policy** NIST Cybersecurity Framework Reference NIST CsF: Mitigation Contained Incidents (RS.MI-1)	To ensure incidents are contained.
118	**Mitigate Incidents Policy** NIST Cybersecurity Framework Reference NIST CsF: Mitigation Mitigate incidents (RS.MI-2)	To ensure incidents are mitigated.
119	**Vulnerabilities Documentation Policy** NIST Cybersecurity Framework Reference NIST CsF: Mitigation Vulnerabilities documentation (RS.MI-3)	To mitigate identified vulnerabilities.

#	NIST Cybersecurity Framework Policy	Policy Description
120	**Improvements (Respond)** NIST Cybersecurity Framework Reference NIST CsF: Improvements (Respond) (RS.IM)	To improve the response plan by incorporating lessons learned from all response activities.
121	**Response Plan Lesson Learned Policy** NIST Cybersecurity Framework Reference Response Plan Lesson Learned (RS.IM-1)	Response plans incorporate lessons learned.
122	**Response Strategies Policy** NIST Cybersecurity Framework Reference NIST CsF: Improvements (Respond) Response Strategies (RS.IM-2)	Response strategies are updated.
123	**Recovery Planning** NIST Cybersecurity Framework Reference NIST CsF: Recovery Planning (RC.RP)	To ensure timely restoration of systems or assets affected by cybersecurity events.
124	**Execute Recovery Plan Policy** NIST Cybersecurity Framework Reference NIST CsF: Recovery Planning Execute Recovery Plan (RC.RP-1)	Recovery plan is executed during or after a cybersecurity incident.
125	**Improvements (Recover)** NIST Cybersecurity Framework Reference NIST Cybersecurity Framework Reference NIST CsF: Improvements (Recover) (RC.IM)	To improve recovery planning and processes by incorporating lessons learned.
126	**Recovery Plan Lesson Learned Policy** NIST Cybersecurity Framework Reference NIST CsF: Improvements (Recover) Recovery Plan Lesson Learned (RC.IM-1)	To improve recovery planning and processes by incorporating lessons learned.
127	**Recovery Strategies Policy** NIST Cybersecurity Framework Reference NIST CsF: Improvements (Recover) Recovery Strategies (RC.IM-2)	To improve recovery planning and processes by incorporating lessons learned.

#	NIST Cybersecurity Framework Policy	Policy Description
128	**Communications (Recover)** NIST Cybersecurity Framework Reference NIST CsF: Improvements (Recover) Recovery Strategies (RC.IM-2)	To communicate recovery activities to internal stakeholders and repair the reputation after an event.
129	**Public Relations Policy** NIST Cybersecurity Framework Reference NIST CsF: Improvements (Recover) Public Relations (RC.CO-1)	Public relations are managed.
130	**Repair Policy** NIST Cybersecurity Framework Reference NIST Cybersecurity Framework Reference NIST CsF: Improvements (Recover) Repair (RC.CO-2)	To ensure the organization's reputation is repaired after an incident.
131	**Recovery Activities Communication Policy** NIST Cybersecurity Framework Reference NIST CsF: Improvements (Recover) Recovery Activities Communication (RC.CO-3)	To communicate recovery activities to management and stakeholders.