NIST CsF Policy Index

#	NIST CsF Policy	Policy Description
1	**Asset Management**	This policy describes the activities required to perform Asset Management.
2	Physical Devices Inventory Policy (NIST CsF ID.AM-1)	This policy describes the physical devices and systems within the organization are inventoried.
3	Software and Application Inventory Policy (NIST CsF ID.AM-2)	This policy describes the software platforms and applications within the organization that are inventoried.
4	Communication and Data Flow Policy (NIST CsF ID.AM-3)	This policy describes that the organizational communication and data flows are mapped.
5	External Information System Catalog Policy (NIST CsF ID.AM-4)	This policy describes that the external information systems are cataloged.
6	Resource Priority Policy (NIST CsF ID.AM-5)	This policy describes the resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.
7	Workforce and Stakeholders Roles and Responsibilities Policy (NIST CsF ID.AM-6)	This policy describes the cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
8	**Business Environment**	This policy describes the organizational cyber security roles and risk management decisions.
9	Supply Chain Policy (NIST CsF ID.BE-1)	This policy describes the organization's role in the supply chain is identified and communicated.
10	Critical Infrastructure Communication Policy (NIST CsF ID.BE-2)	This policy describes the organization's place in critical infrastructure and its industry sector is identified and communicated.
11	Organizational Mission, Objectives, and Activities Policy (NIST CsF ID.BE-3)	This policy describes the priorities for organizational mission, objectives, and activities are established and communicated.
12	Critical Services Delivery Policy (NIST CsF ID.BE-4)	This policy describes the dependencies and critical functions for delivery of critical services are established.
13	Critical Services Delivery Support Policy (NIST CsF ID.BE-5)	This policy describes the resilience requirements to support delivery of critical services are established for all operating states

#	NIST CsF Policy	Policy Description
		(e.g. under duress/attack, during recovery, normal operations).
14	**Governance**	This policy describes the organizational policies, processes, and procedures for information security and risk management.
15	Cybersecurity Policy (NIST CsF ID.GV-1)	This policy describes the organizational cybersecurity policy is established and communicated.
16	External Partners Cybersecurity Roles and Responsibilities Policy (NIST CsF ID.GV-2)	This policy describes the cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.
17	Cybersecurity Legal and Regulatory Requirements Policy (NIST CsF ID.GV-3)	This policy describes the legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
18	Governance and Risk Management Policy (NIST CsF ID.GV-4)	This policy describes the governance and risk management process.
19	**Risk Assessment**	This policy describes the identify the organizational asset vulnerabilities and cybersecurity risk to operations.
20	Asset Vulnerabilities Policy (NIST CsF ID.RA-1)	This policy describes the asset vulnerabilities are identified and documented.
21	Cyber Threat Intelligence Policy (NIST CsF ID.RA-2)	This policy describes the cyber threat intelligence received from information sharing forums and sources.
22	External and Internal Threats Policy (NIST CsF ID.RA-3)	This policy describes the threats, both internal and external, are identified and documented.
23	Potential Business Impacts Policy (NIST CsF ID.RA-4)	This policy describes the potential business impacts and likelihoods are identified.
24	Determining Risk Policy (NIST CsF ID.RA-5)	This policy describes the threats, vulnerabilities, likelihoods, and impacts that are used to determine risk.
25	Prioritize Risk Responses Policy (NIST CsF ID.RA-6)	This policy describes the risk responses that are identified and prioritized.

#	NIST CsF Policy	Policy Description
26	**Risk Management Strategy**	This policy describes the organizational risk tolerance and established operational risk decisions.
27	Risk Management Process Policy (NIST CsF ID.RM-1)	This policy describes the risk management processes that are established, managed, and agreed to by organizational stakeholders.
28	Determine Risk Tolerance Policy (NIST CsF ID.RM-2)	This policy describes the organizational risk tolerance is determined and clearly expressed.
29	Risk Tolerance Policy (NIST CsF ID.RM-3)	This policy describes the organization's determination of risk tolerance informed by its role in critical infrastructure and sector specific risk analysis.
30	**Supply Chain Risk Management**	This policy describes the identify the process for supply chain risk management and to implement contract with suppliers and third-party partners.
31	Supply Chain Risk Management Processes Policy (NIST CsF ID.SC-1)	This policy describes the cyber supply chain risk management processes identified, established, assessed, managed, and agreed to by organizational stakeholders.
32	Third Party Services Policy (NIST CsF ID.SC-2)	This policy describes the suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.
33	Cyber Supply Chain Risk Management Plan Policy (NIST CsF ID.SC-3)	This policy describes the contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
34	Audit Third Party Partners Policy (NIST CsF ID.SC-4)	This policy describes the suppliers and third-party partners routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
35	Response and Recovery Plan Testing Policy (NIST CsF ID.SC-5)	This policy describes the response and recovery planning and testing are conducted with suppliers and third-party providers.

#	NIST CsF Policy	Policy Description
36	**Identity Management, Authentication and Access Control**	This policy describes the management for limited access to facilities and organization assets.
37	Identity Management Policy (NIST CsF PR.AC-1)	This policy describes the identities and credentials issued, managed, verified, revoked, and audited for authorized devices, users and processes.
38	Access Management for Assets Policy (NIST CsF PR.AC-2)	This policy describes the physical access to assets are managed and protected.
39	Remote Access Management Policy (NIST CsF PR.AC-3)	This policy describes the remote access managed.
40	Access Authorization Policy (NIST CsF PR.AC-4)	This policy describes the access permissions and authorizations that are managed, incorporating the principles of least privilege and separation of duties.
41	Network Integrity Policy (NIST CsF PR.AC-5)	This policy describes the network integrity is protected (e.g., network segregation, network segmentation).
42	Proofed Identities Policy (NIST CsF PR.AC-6)	This policy describes the identities that are proofed and bound to credentials and asserted in interactions.
43	Authentication Policy (NIST CsF PR.AC-7)	This policy describes the users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
44	**Awareness and Training**	This policy describes the cyber security awareness and training to organizational personnel covering their jobs and responsibilities.
45	User Training Policy (NIST CsF PR.AT-1)	This policy describes that all users are informed and trained.
46	Privileged Users Policy (NIST CsF PR.AT-2)	This policy describes the privileged users understand their roles and responsibilities.
47	Third Party Stakeholders Policy (NIST CsF PR.AT-3)	This policy describes the third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.

#	NIST CsF Policy	Policy Description
48	Senior Executives Responsibilities Policy (NIST CsF PR.AT-4)	This policy describes the senior executives understand their roles and responsibilities.
49	Cybersecurity Personnel's Responsibilities Policy (NIST CsF PR.AT-5)	This policy describes the physical and cybersecurity personnel understand their roles and responsibilities.
50	**Data Security**	This policy describes the risk strategy to ensure the confidentiality, integrity, and availability (CIA) of information assets.
51	Data at Rest Policy (NIST CsF PR.DS-1)	This policy describes that data-at-rest is protected.
52	Data in Transit Policy (NIST CsF PR.DS-2)	This policy describes that data-in-transit is protected.
53	Asset Management and Disposition Policy (NIST CsF PR.DS-3)	This policy describes that assets are formally managed throughout removal, transfers, and disposition.
54	Availability Policy (NIST CsF PR.DS-4)	This policy describes the adequate capacity to ensure availability is maintained.
55	Data Leaks Protection Policy (NIST CsF PR.DS-5)	This policy describes the protections against data leaks are implemented.
56	Integrity Checking Mechanisms Policy (NIST CsF PR.DS-6)	This policy describes the integrity checking mechanisms used to verify software, firmware, and information integrity.
57	Segregation in Development and Testing Environment(s) Policy (NIST CsF PR.DS-7)	This policy describes the development and testing environment(s) separate from the production environment.
58	Hardware Integrity Policy (NIST CsF PR.DS-8)	This policy describes the integrity checking mechanism used to verify hardware integrity.
59	**Information Protection Processes and Procedures**	This policy describes that maintain policies, processes, and procedures to manage protection of information systems and assets.
60	Baseline Configuration Policy (NIST CsF PR.IP-1)	This policy describes the baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).

#	NIST CsF Policy	Policy Description
61	System Development Life Cycle Policy (NIST CsF PR.IP-2)	This policy describes the System Development Life Cycle to manage systems is implemented.
62	Configuration Change Control Policy (NIST CsF PR.IP-3)	This policy describes the configuration change control processes in place.
63	Backup Management Policy (NIST CsF PR.IP-4)	This policy describes that backups of information are conducted, maintained, and tested.
64	Physical Operating Environment Policy (NIST CsF PR.IP-5)	This policy describes the policy and regulations regarding the physical operating environment for organizational assets are met.
65	Disposal Policy (NIST CsF PR.IP-6)	This policy describes that the data is destroyed according to policy.
66	Protection Improvement Policy (NIST CsF PR.IP-7)	This policy describes that the protection processes are improved.
67	Protection Technologies Policy (NIST CsF PR.IP-8)	This policy describes that the effectiveness of protection technologies is shared.
68	Response Plans Availability Policy (NIST CsF PR.IP-9)	This policy describes that the response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
69	Testing of Response and Recovery Plans Policy (NIST CsF PR.IP-10)	This policy describes that the response and recovery plans are tested.
70	Cybersecurity and Human Resources Policy (NIST CsF PR.IP-11)	This policy describes the cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).
71	Vulnerability Management Policy (NIST CsF PR.IP-12)	This policy describes the vulnerability management plan developed and implemented.
72	**Maintenance**	This policy describes to maintain policies and procedures for the maintenance and repairs of organizational assets.
73	Asset Maintenance and Repair Policy (NIST CsF PR.MA-1)	This policy describes the maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
74	Remote Maintenance Policy (NIST CsF PR.MA-2)	This policy describes the remote maintenance of organizational assets is approved, logged,

#	NIST CsF Policy	Policy Description
		and performed in a manner that prevents unauthorized access.
75	**Protective Technology**	This policy describes the technical security solutions to ensure the security and protection of systems and organizational assets.
76	Audit Records Management Policy (NIST CsF PR.PT-1)	This policy describes the audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
77	Removable Media Protection Policy (NIST CsF PR.PT-2)	This policy describes that the removable media is protected and its use restricted according to policy.
78	Configuring Essential Capabilities Policy (NIST CsF PR.PT-3)	This policy describes the principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
79	Network Protection Policy (NIST CsF PR.PT-4)	This policy describes the communications and control networks are protected.
80	Mechanism to Achieve Resilience Requirements Policy (NIST CsF PR.PT-5)	This policy describes the mechanisms (e.g., failsafe, load balancing, hot swap) implemented to achieve resilience requirements in normal and adverse situations.
81	**Anomalies and Events**	This policy describes the detection of anomalous activities and events in a timely manner.
82	Network Operations Baseline Policy (NIST CsF DE.AE-1)	This policy describes the baseline of network operations and expected data flows for users and systems established and managed.
83	Event Detection and Analysis Policy (NIST CsF DE.AE-2)	This policy describes that the detected events are analyzed to understand the attack targets and methods.
84	Event Data Collection Policy (NIST CsF DE.AE-3)	This policy describes the event data collected and correlated from multiple sources and sensors.
85	Event's Impact Policy (NIST CsF DE.AE-4)	This policy describes that the impact of events is determined.
86	Incident Notification Policy (NIST CsF DE.AE-5)	This policy describes the incident alert thresholds established.

#	NIST CsF Policy	Policy Description
87	**Security Continuous Monitoring**	This policy describes the monitoring of the physical environment and information system and assets at discrete intervals to identify cybersecurity events.
88	Network Monitoring Policy (NIST CsF DE.CM-1)	This policy describes the network monitored to detect potential cybersecurity events.
89	Physical Environment Monitoring Policy (NIST CsF DE.CM-2)	This policy describes the physical environment is monitored to detect potential cybersecurity events.
90	Personnel Activity Monitoring Policy (NIST CsF DE.CM-3)	This policy describes the personnel activity is monitored to detect potential cybersecurity events.
91	Malicious Code Detection Policy (NIST CsF DE.CM-4)	This policy describes the malicious code is detected.
92	Unauthorized Mobile Code Detection Policy (NIST CsF DE.CM-5)	This policy describes the unauthorized mobile code is detected.
93	External Service Provider Activity Monitoring Policy (NIST CsF DE.CM-6)	This policy describes that the external service provider activity is monitored to detect potential cybersecurity events.
94	Software and Device Monitoring Policy (NIST CsF DE.CM-7)	This policy describes the monitoring for unauthorized personnel, connections, devices, and software performed.
95	Vulnerability Scans Policy (NIST CsF DE.CM-8)	This policy describes the vulnerability scans that are performed.
96	**Detection Processes**	This policy describes the awareness on anomalous events and test detection activities.
97	Event Detection Roles and Responsibilities Policy (NIST CsF DE.DP-1)	This policy describes the roles and responsibilities for detection that are well defined to ensure accountability.
98	Detection Activities Policy (NIST CsF DE.DP-2)	This policy describes the detection activities comply with all applicable requirements.
99	Detection Process Test Policy (NIST CsF DE.DP-3)	This policy describes the detection processes are tested.
100	Event Communication Policy (NIST CsF DE.DP-4)	This policy describes the event detection information is communicated.

#	NIST CsF Policy	Policy Description
101	Detection Process Improvement Policy (NIST CsF DE.DP-5)	This policy describes the detection processes are continuously improved.
102	**Response Planning**	This policy describes the maintain a response plan to ensure timely response to detected cybersecurity events.
103	Execute Response Plan Policy (NIST CsF RS.RP-1)	This policy describes the response plan is executed during or after an incident.
104	**Communications (Respond)**	This policy describes the coordinate response activities with stakeholders consistently to achieve broader cybersecurity situational awareness.
105	Response Roles and Responsibilities Policy (NIST CsF RS.CO-1)	This policy describes the personnel know their roles and order of operations when a response needed.
106	Reporting Incident Policy (NIST CsF RS.CO-2)	This policy describes the incidents are reported consistent with established criteria.
107	Response Plan Policy (NIST CsF RS.CO-3)	This policy describes that the information is shared consistent with response plans.
108	Response Plan Policy (NIST CsF RS.CO-4)	This policy describes the coordination with stakeholders occurs consistent with response plans.
109	Cybersecurity Awareness for Stakeholders Policy (NIST CsF RS.CO-5)	This policy describes the voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
110	**Analysis**	This policy describes the conduct analysis to understand response and recovery activities.
111	Notification Investigation Policy (NIST CsF RS.AN-1)	This policy describes the notifications from detection systems are investigated.
112	Understanding incident Impact Policy (NIST CsF RS.AN-2)	This policy describes that the impact of the incident is understood.
113	Incident Forensics Policy (NIST CsF RS.AN-3)	This policy describes the forensics are performed.
114	Incidents Categorization Policy (NIST CsF RS.AN-4)	This policy describes the incidents are categorized consistent with response plans.

#	NIST CsF Policy	Policy Description
115	Internal and External Vulnerability Policy (NIST CsF RS.AN-5)	This policy describes the processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).
116	**Mitigation**	This policy describes the perform activities to mitigate incident and newly identified vulnerabilities.
117	Contained Incidents Policy (NIST CsF RS.MI-1)	This policy describes that the incidents are contained.
118	Mitigate Incidents Policy (NIST CsF RS.MI-2)	This policy describes the incidents are mitigated.
119	Vulnerabilities Documentation Policy (NIST CsF RS.MI-3)	This policy describes the newly identified vulnerabilities are mitigated or documented as accepted risks.
120	**Improvements (Respond)**	This policy describes the improve the response plan by incorporating lessons learned from all response activities.
121	Response Plan Lesson Learned Policy (NIST CsF RS.IM-1)	This policy describes the response plans incorporate lessons learned.
122	Response Strategies Policy (NIST CsF RS.IM-2)	This policy describes the response strategies are updated.
123	**Recovery Planning**	This policy describes the timely restoration of systems or assets affected by cybersecurity events.
124	Execute Recovery Plan Policy (NIST CsF RC.RP-1)	This policy describes that recovery plan is executed during or after a cybersecurity incident.
125	**Improvements (Recover)**	This policy describes the improve recovery planning and processes by incorporating lessons learned.
126	Recovery Plan Lesson Learned Policy (NIST CsF RC.IM-1)	This policy describes the recovery plans incorporate lessons learned.
127	Recovery Strategies Policy (NIST CsF RC.IM-2)	This policy describes the recovery strategies are updated.

#	NIST CsF Policy	Policy Description
128	**Communications (Recover)**	This policy describes the communicate recovery activities to internal stakeholders and repair the reputation after an event.
129	Public Relations Policy (NIST CsF RC.CO-1)	This policy describes that the public relations are managed.
130	Repair Policy (NIST CsF RC.CO-2)	This policy describes that the reputation is repaired after an incident.
131	Recovery Activities Communication Policy (NIST CsF RC.CO-3)	This policy describes the recovery activities are communicated to internal and external stakeholders as well as executive and management teams.