| # | NIST Cybersecurity Framework v2.0 Policy | Policy Description |
|---|---|---|
| 1 | **Organizational Context Policy**<br><br>NIST Cybersecurity Framework Reference NIST CSF: Organizational Context (GV.OC) | Establishes a framework for aligning cybersecurity strategies and practices with the organization's mission, objectives, and business environment. It is designed to ensure that cybersecurity initiatives support and enhance the organization's operational effectiveness, stakeholder requirements, and compliance with relevant legal and regulatory standards. |
| 2 | **Risk Management Strategy Policy**<br><br>NIST Cybersecurity Framework Reference NIST CSF: Risk Management Strategy (GV.RM) | Establishes the organization's approach to comprehensive cybersecurity risk management. It is designed to align with the organization's mission, objectives, and risk tolerance, encompassing a full spectrum of cybersecurity threats, vulnerabilities, and potential impacts. |
| 3 | **Cybersecurity Supply Chain Risk Management Policy**<br><br>NIST Cybersecurity Framework Reference NIST CSF: Cybersecurity Supply Chain Risk Management (GV.SC) | Establishes guidelines for identifying, assessing, and managing cybersecurity risks associated with the organization's supply chain. It aims to integrate supply chain risks into the overall cybersecurity risk management framework, ensuring the security and resilience of the organization's operations and assets. |
| 4 | **Cybersecurity Roles, Responsibilities, and Authorities Policy**<br><br>NIST Cybersecurity Framework Reference NIST CSF: Roles, Responsibilities, and Authorities (GV.RR) | Outline the specific roles, responsibilities, and authorities within the organization regarding cybersecurity. It aims to ensure clarity and efficiency in managing cybersecurity risks, aligning with the organization's strategic objectives and compliance requirements. |
| 5 | **Cybersecurity Policies, Processes, and Procedures Policy (GV.PO)**<br><br>NIST Cybersecurity Framework Reference NIST CSF: Policies, Processes, and Procedures (GV.PO) | Outlines the organization's commitment to developing, implementing, and maintaining comprehensive cybersecurity policies, processes, and procedures. These guidelines are designed to protect the organization's information assets and support its business objectives, operational goals, and compliance requirements. |
| 6 | **Cybersecurity Oversight Policy**<br><br>NIST Cybersecurity Framework Reference NIST CSF: Oversight (GV.OV) | Outlines the framework for executive and board-level oversight of the organization's cybersecurity efforts. It aims to ensure that senior leaders are actively involved in guiding and reviewing the organization's cybersecurity strategy and practices, aligning them with the |

| # | NIST Cybersecurity Framework v2.0 Policy | Policy Description |
|---|---|---|
| | | overall business objectives and risk management. |
| 7 | **Asset Management Policy**<br><br>NIST Cybersecurity Framework Reference<br>NIST CSF: Asset Management (ID.AM) | Establishes the framework for effective management of all physical and digital assets within the organization. It aims to maintain an accurate inventory of assets, ensure their proper classification, and integrate their management into the organization's overall cybersecurity strategy. |
| 8 | **Cybersecurity Risk Assessment Policy**<br><br>NIST Cybersecurity Framework Reference<br>NIST CSF: Risk Assessment (ID.RA) | Establishes a structured approach for conducting comprehensive cybersecurity risk assessments within the organization. It aims to identify, analyze, and prioritize risks to the organization's information systems and assets, ensuring that these risks are managed effectively in line with the organization's overall cybersecurity strategy. |
| 9 | **Cybersecurity Improvement Policy**<br><br>NIST Cybersecurity Framework Reference<br>NIST CSF: Improvement (ID.IM) | Establishes a framework for the continuous improvement of the organization's cybersecurity practices. It focuses on regularly updating and enhancing cybersecurity measures to adapt to evolving threats, technological advancements, and changes in the business environment. |
| 10 | **Identity Management, Authentication, and Access Control Policy**<br><br>NIST Cybersecurity Framework Reference<br>NIST CSF: Identity Management, Authentication, and Access Control (PR.AA) | Establishes the framework for effective identity management, authentication, and access control within the organization. It aims to ensure that access to organizational systems and data is secure, controlled, and aligned with the individual's role and responsibilities. |
| 11 | **Cybersecurity Awareness and Training Policy**<br><br>NIST Cybersecurity Framework Reference<br>NIST CSF: Awareness and Training (PR.AT) | Establishes a comprehensive approach to cybersecurity awareness and training within the organization. It aims to equip all employees with the knowledge and skills necessary to protect organizational assets and information against cybersecurity threats. |
| 12 | **Data Security Policy**<br><br>NIST Cybersecurity Framework Reference<br>NIST CSF: Data Security (PR.DS) | Establishes the framework for safeguarding the organization's data against unauthorized access, use, disclosure, disruption, modification, or destruction. It aims to protect data at rest, in transit, and during processing, in |

| # | NIST Cybersecurity Framework v2.0 Policy | Policy Description |
|---|---|---|
| | | compliance with applicable laws and regulations. |
| 13 | **Platform Security Policy**<br><br>NIST Cybersecurity Framework Reference<br>NIST CSF: Platform Security (PR.PS) | Establishes the organization's commitment to securing all its computing platforms, including operating systems, applications, and network devices, to protect against cybersecurity threats and vulnerabilities. |
| 14 | **Technology Infrastructure Resilience Policy**<br><br>NIST Cybersecurity Framework Reference<br>NIST CSF: Technology Infrastructure Resilience (PR.IR) | Establishes guidelines for ensuring the resilience of the organization's technology infrastructure. It aims to maintain continuity of critical services and rapid recovery from system disruptions, thus safeguarding the organization's operational capabilities. |
| 15 | **Continuous Monitoring Policy**<br><br>NIST Cybersecurity Framework Reference<br>NIST CSF: Continuous Monitoring (DE.CM) | Establishes the framework for continuous monitoring of the organization's networks, systems, and data to detect and respond to cybersecurity threats. It aims to ensure proactive identification of potential security incidents and anomalies in real-time. |
| 16 | **Adverse Event Analysis Policy**<br><br>NIST Cybersecurity Framework Reference<br>NIST CSF: Adverse Event Analysis (DE.AE) | Provides guidelines for the effective detection, analysis, and management of adverse cybersecurity events. It aims to ensure that such events are identified promptly, analyzed accurately, and addressed appropriately to mitigate potential security risks. |
| 17 | **Incident Management Policy**<br><br>NIST Cybersecurity Framework Reference<br>NIST CSF: Incident Management (RS.MA) | Establishes guidelines for effectively managing cybersecurity incidents within the organization. It aims to ensure a coordinated and prompt response to incidents, minimizing their impact and facilitating a swift return to normal operations. |
| 18 | **Incident Analysis Policy**<br><br>NIST Cybersecurity Framework Reference<br>NIST CSF: Incident Analysis (RS.AN) | Outlines the organization's approach to the analysis of cybersecurity incidents. It emphasizes the importance of immediate, thorough investigation to understand, mitigate, and prevent cybersecurity incidents. |
| 19 | **Incident Response Reporting and Communication Policy** | Outline the procedures for reporting and communicating about cybersecurity incidents within the organization. It aims to ensure timely, accurate, and effective communication both |

| # | NIST Cybersecurity Framework v2.0 Policy | Policy Description |
|---|---|---|
| | NIST Cybersecurity Framework Reference NIST CSF: Incident Response Reporting and Communication (RS.CO) | internally and externally, in compliance with legal and regulatory requirements. |
| 20 | **Incident Mitigation Policy**<br><br>NIST Cybersecurity Framework Reference NIST CSF: Incident Mitigation (RS.MI) | Establishes the organization's approach to effectively mitigating cybersecurity incidents, aimed at rapidly containing, eradicating, and recovering from such incidents to minimize their impact on operations and data integrity. |
| 21 | **Incident Recovery Plan Execution Policy**<br><br>NIST Cybersecurity Framework Reference NIST CSF: Incident Recovery Plan Execution (RC.RP) | Outlines the organization's approach to executing the Incident Recovery Plan following a cybersecurity incident. It emphasizes the timely and efficient restoration of systems and services to minimize operational disruption and data loss. |
| 22 | **Incident Recovery Communication Policy**<br><br>NIST Cybersecurity Framework Reference NIST CSF: Incident Recovery Communication (RC.CO) | Defines the approach for communication during and after the recovery phase of a cybersecurity incident. It aims to ensure that all communication is clear, timely, and effective, thereby maintaining trust and confidence among internal and external stakeholders. |