NIST FUNCTION:

Identify

Identify: **Asset Management** (ID.AM)

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

1. Acceptable Use of Information Technology Resource Policy
2. Access Control Policy
3. Account Management/Access Control Standard
4. Identification and Authentication Policy Information
5. Security Policy Security Assessment and Authorization Policy
6. Security Awareness and Training Policy

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

1. Acceptable Use of Information Technology Resource Policy
2. Access Control Policy
3. Account Management/Access Control Standard
4. Identification and Authentication Policy
5. Information Security Policy
6. Security Assessment and Authorization Policy
7. Security Awareness and Training Policy

ID.AM.4 **External information systems are catalogued.**

1. System and Communications Protection Policy

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

1. Information Classification Standard
2. Information Security Policy

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

1. Acceptable Use of Information Technology Resource Policy
2. Information Security Policy
3. Security Awareness and Training Policy

Identify: Risk Management Strategy (ID.RM)

ID.RM.1 **Risk management processes are established, managed, and agreed to by organizational stakeholders.**

1. Information Security Policy
2. Information Security Risk Management Standard
3. Risk 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.**

1. Identification and Authentication Policy
2. Security Assessment and Authorization Policy
3. Systems and Services Acquisition 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.**

1. Identification and Authentication Policy
2. Security Assessment and Authorization Policy
3. Systems and Services Acquisition Policy

ID.SC.5 **Response and recovery planning and testing are conducted with suppliers and third-party providers. Computer Security Threat Response Policy Cyber Incident Response Standard Incident Response Policy Systems and Services Acquisition Policy.**

Protect

Protect: Identity Management and Access Control (PR.AC)

PR.AC.1 **Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.**

1. Access Control Policy
2. Account Management/Access Control Standard
3. Authentication Tokens Standard

4. Configuration Management Policy
5. Identification and Authentication Policy
6. Sanitization Secure Disposal Standard
7. Secure Configuration Standard
8. Secure System Development Life Cycle Standard

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

1. Remote Access Standard

PR.AC.4 **Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.**

2. Access Control Policy
3. Account Management/Access Control Standard
4. Authentication Tokens Standard
5. Configuration Management Policy
6. Identification and Authentication Policy
7. Sanitization Secure Disposal Standard
8. Secure Configuration Standard
9. Secure System Development Life Cycle Standard

PR.AC.5 **Network integrity is protected (e.g., network segregation, network segmentation).**

1. 802.11 Wireless Network Security Standard
2. Mobile Device Security
3. System and Information Integrity Policy
4. Protect: Awareness and Training (PR.AT)

PR.AT.1 **All users are informed and trained.**

1. Acceptable Use of Information Technology Resources Policy
2. Information Security Policy
3. Personnel Security Policy
4. Physical and Environmental Protection Policy
5. Security Awareness and Training Policy

Protect: **Data Security** (PR.DS)

PR.DS.1 **Data-at-rest is protected**

1. Computer Security Threat Response Policy

2. Cyber Incident Response Standard
3. Encryption Standard
4. Incident Response Policy
5. Information Security Policy
6. Maintenance Policy
7. Media Protection Policy
8. Mobile Device Security
9. Patch Management Standard

PR.DS.2 **Data-in-transit is protected.**

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Encryption Standard
4. Incident Response Policy
5. Information Security Policy
6. Maintenance Policy
7. Media Protection Policy
8. Mobile Device Security
9. Patch Management Standard

PR.DS.3 **Assets are formally managed throughout removal, transfers, and disposition**.

1. Access Control Policy
2. Account Management/Access Control Standard
3. Authentication Tokens Standard
4. Configuration Management Policy
5. Identification and Authentication Policy
6. Sanitization Secure Disposal Standard
7. Secure Configuration Standard Secure System Development Life Cycle Standard

PR.DS.8 **Integrity checking mechanisms are used to verify hardware integrity.**

1. System and Information Integrity Policy

Protect: **Information Protection Processes and Procedures (PR.IP)**

PR.IP.1 **A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).**

1. Access Control Policy
2. Account Management/Access Control Standard
3. Authentication Tokens Standard
4. Configuration Management Policy
5. Identification and Authentication Policy
6. Sanitization Secure Disposal Standard Secure Configuration Standard
7. Secure System Development Life Cycle Standard

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

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Encryption Standard
4. Incident Response Policy
5. Information Security Policy
6. Maintenance Policy
7. Media Protection Policy
8. Mobile Device Security
9. Patch Management Standard

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

1. Maintenance Policy
2. Media Protection Policy
3. Sanitization Secure Disposal Standard

PR.IP.9 **Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed**.

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy
4. Planning Policy

PR.IP.10 **Response and recovery plans are tested.**

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy
4. Planning 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.**

1. Maintenance Policy
2. Remote Access Standard
3. Security Logging Standard

Protect: **Protective Technology** (PR.PT)

PR.PT.1 **Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.**

1. Access Control Policy
2. Account Management/Access Control Standard
3. Authentication Tokens Standard
4. Configuration Management Policy
5. Identification and Authentication Policy
6. Sanitization Secure Disposal Standard
7. Secure Configuration Standard
8. Secure System Development Life Cycle Standard
9. Security Logging Standard

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

1. Acceptable Use of Technology Resources Policy
2. Media Protection Policy
3. Mobile Device Security

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

1. Encryption Standard
2. Information Security Policy
3. Maintenance Policy
4. Media Protection Policy
5. Mobile Device Security
6. System and Communications Protection Policy

Detect

Detect: **Anomalies and Events** (DE.AE)

DE.AE.3 **Event data are collected and correlated from multiple sources and sensors.**

1. Auditing and Accountability Standard
2. Security Logging Standard
3. System and Information Integrity Policy
4. Vulnerability Scanning Standard

Detect: **Security Continuous Monitoring** (DE.CM)

DE.CM.1 **The network is monitored to detect potential cybersecurity events.**

1. Encryption Standard
2. Information Security Policy
3. Maintenance Policy
4. Media Protection Policy
5. Mobile Device Security
6. Patch Management Standard
7. Security Assessment and Authorization Policy
8. Vulnerability Scanning Standard

DE.CM.4 **Malicious code is detected.**

1. Auditing and Accountability Standard
2. Secure Coding Standard
3. Security Logging Standard
4. System and Information Integrity Policy
5. Vulnerability Scanning Standard

DE.CM.7 **Monitoring for unauthorized personnel, connections, devices, and software is performed.**

1. Auditing and Accountability Standard
2. Security Logging Standard
3. System and Information Integrity Policy
4. Vulnerability Scanning Standard

Detect: **Detection Processes** (DE.DP)

DE.DP.1 **Roles and responsibilities for detection are well defined to ensure accountability.**

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy
4. Information Security Policy

DE.DP.4 **Event detection information is communicated.**

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy
4. Information Security Policy

Respond

Respond: **Response Planning** (RS.RP)

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

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy
4. Planning Policy

Respond: **Communications** (RS.CO)

RS.CO.1 **Personnel know their roles and order of operations when a response is needed.**

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy

RS.CO.2 **Incidents are reported consistent with established criteria**.

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy

RS.CO.3 **Information is shared consistent with response plans.**

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy

RS.CO.4 **Coordination with stakeholders occurs consistent with response plans**

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy

RS.CO.5 **Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.**

1. Computer Security Threat Response Policy Cyber
2. Incident Response Standard
3. Incident Response Policy

Respond: **Analysis** (RS.AN)

RS.AN.4 **Incidents are categorized consistently with response plans**.

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy

Respond: **Improvements** (RS.IM)

RS.IM.1 **Response plans incorporate lessons learned.**

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy

RS.IM.2 Response strategies are updated.

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy

Recover

Recover: **Recovery Planning** (RC.RP)

RC.RP.1 **Recovery plan is executed during or after a cybersecurity incident.**

1. Computer Security Threat Response Policy
2. Contingency Planning Policy
3. Cyber Incident Response Standard

4. Incident Response Policy

Recover: **Improvements** (RC.IM)

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

1. Computer Security Threat Response Policy
2. Contingency Planning Policy
3. Cyber Incident Response Standard
4. Incident Response Policy

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

1. Computer Security Threat Response Policy
2. Contingency Planning Policy
3. Cyber Incident Response Standard
4. Incident Response Policy

Recover: **Communications** (RC.CO)

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

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy

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

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Policy

RC.CO.3 **Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.**

1. Computer Security Threat Response Policy
2. Cyber Incident Response Standard
3. Incident Response Polic