Cybersecurity Policy for Manufacturing - Low Risk Environment

1. Introduction

This Cybersecurity Policy outlines the necessary measures to protect the confidentiality, integrity, and availability of information and systems within our manufacturing environment. While we operate in a defined "Low Risk" environment, meaning a limited impact would result from a successful cyberattack due to the nature of our operations and data processed, a proactive security posture remains essential for business continuity and regulatory compliance. This policy applies to all employees, contractors, vendors, and any other individuals accessing or using company information systems and data, regardless of location or device. This policy aligns with the Risk Management Framework (RMF) and other relevant industry best practices.

2. Risk Assessment

A risk assessment will be conducted annually, or more frequently if significant changes occur in the business environment, technology landscape, or threat landscape. This assessment will identify potential threats, vulnerabilities, and the likelihood and impact of potential security incidents. The scope of the risk assessment will include all systems, networks, and data involved in manufacturing operations, with a focus on those identified as critical assets.

--Specific Considerations for Low Risk Environments:--

- --Simplified Approach:-- Risk assessments will utilize a streamlined methodology, focusing on identifying readily apparent vulnerabilities and common threats. The methodology will be documented and consistently applied.
- --Asset Prioritization:-- Resources will be prioritized towards protecting the most critical assets, even within a low-risk context. Examples include systems controlling physical machinery or containing sensitive customer information (if applicable).
- --Thresholds:-- The risk assessment will establish acceptable risk thresholds, providing a clear benchmark for determining the necessity of implementing new security controls. Any risk exceeding the threshold will trigger a documented remediation plan with clearly defined responsibilities and timelines.

3. Data Protection

All data, including manufacturing process data, customer information (if applicable), and employee records, must be protected against unauthorized access, disclosure, and modification.

--Specific Requirements:--

- --Data Classification:-- Data will be classified based on its sensitivity and criticality. While this is a low-risk environment, basic classifications (e.g., Public, Internal, Confidential) will be applied to guide data handling practices. A Data Classification Guide will be maintained to define the criteria for each classification level.
- --Data Encryption:-- Sensitive data at rest (e.g., on servers, laptops) will be encrypted using industry-standard encryption algorithms. Data in transit (e.g., during network

transmission) will also be encrypted where feasible and practical. The choice of algorithms and key management practices will be documented.

- --Data Backup and Recovery:-- Regular backups of critical data will be performed and stored securely, both on-site and off-site, to ensure business continuity in the event of a disaster or data loss. Backup schedules will be appropriate for the RTO/RPO goals defined as part of the low risk profile. Backup media shall be verified for integrity through periodic test restores.
- --Data Retention and Disposal:-- Data will be retained only for as long as necessary for business or legal requirements and then securely disposed of to prevent unauthorized access. This includes secure wiping of hard drives and proper disposal of physical media. A data retention schedule will be documented and implemented.

4. Access Controls

Access to information systems and data will be restricted based on the principle of least privilege. Users will only be granted the access necessary to perform their job duties.

--Specific Requirements:--

- --User Account Management:-- User accounts will be created, managed, and terminated according to a defined process. Strong passwords will be enforced, and multi-factor authentication (MFA) will be implemented where feasible, especially for privileged accounts and remote access. This process will include regular reviews of user accounts for accuracy and necessity.
- --Role-Based Access Control (RBAC):-- Access permissions will be assigned based on roles, ensuring that users only have access to the resources required for their specific job functions. Roles and associated permissions will be documented and reviewed periodically.
- --Remote Access:-- Remote access to the network will be secured using VPNs and MFA. Regular reviews of remote access privileges will be conducted. The remote access solution will be regularly patched and updated.
- --Physical Security:-- Physical access to servers, network equipment, and other critical infrastructure will be restricted to authorized personnel. Physical access logs will be maintained and reviewed regularly.

5. Incident Response

A documented incident response plan will be maintained and regularly tested to ensure a coordinated and effective response to security incidents.

--Specific Requirements:--

- --Incident Reporting:-- All suspected security incidents must be reported immediately to the designated security contact(s) using the established reporting channels. Reporting channels will be clearly communicated to all personnel.
- --Incident Response Team:-- An incident response team will be identified and trained to handle security incidents. Roles and responsibilities within the incident response team will be clearly defined.
- --Incident Containment, Eradication, and Recovery:-- The incident response plan will outline procedures for containing, eradicating, and recovering from security incidents.

These procedures will include specific steps for common types of incidents.

- --Post-Incident Analysis:-- Following a security incident, a post-incident analysis will be conducted to identify the root cause of the incident and implement measures to prevent similar incidents from occurring in the future. Findings and recommendations from the post-incident analysis will be documented.
- --Communication Plan:-- Clear communication channels will be established for informing stakeholders about security incidents, including employees, management, and customers (if applicable). This plan will include escalation procedures and pre-approved communication templates.

6. Security Awareness Training

All employees will receive regular security awareness training to educate them about cybersecurity threats and best practices.

--Specific Requirements:--

- --Training Content:-- Training will cover topics such as phishing awareness, password security, data handling, and incident reporting. Training content will be regularly updated to reflect current threats and best practices.
- --Training Frequency:-- Security awareness training will be conducted at least annually, and more frequently for high-risk roles. Refresher training or targeted training may be provided based on identified needs.
- --Training Delivery:-- Training will be delivered through a variety of methods, such as online modules, workshops, and simulations. The effectiveness of training methods will be evaluated periodically.
- --Phishing Simulations:-- Periodic phishing simulations will be conducted to test employees' ability to identify and report phishing emails. Results of phishing simulations will be used to improve training content and identify individuals who may benefit from additional training.

7. Compliance and Auditing

This Cybersecurity Policy will be reviewed and updated at least annually to ensure compliance with applicable laws, regulations, and industry best practices, including the Risk Management Framework (RMF).

--Specific Requirements:--

- --Regular Audits:-- Periodic security audits will be conducted to assess the effectiveness of security controls and identify areas for improvement. Audit scope will be defined based on risk assessments and regulatory requirements.
- --Vulnerability Management:-- Regular vulnerability scanning will be performed to identify and remediate vulnerabilities in systems and applications. Vulnerability scan results will be reviewed and prioritized based on severity and potential impact.
- --Configuration Management:-- Secure configurations will be established and maintained for all systems and devices. Configuration settings will be documented and regularly reviewed to ensure compliance with security best practices.
- --Logging and Monitoring:-- Security logs will be collected and monitored to detect and

investigate security incidents. Log retention policies will be defined and implemented.

- --Continuous Improvement:-- The security program will be continuously improved based on audit findings, vulnerability assessments, and threat intelligence. A formal process for tracking and resolving identified issues will be established.
- --RMF Alignment:-- The RMF will be utilized as a framework for selecting, implementing, and assessing security controls. Even within a low-risk environment, controls will be chosen and tailored to address specific risks and vulnerabilities identified during the risk assessment process. Documentation of control implementation and assessment will be maintained. Deviation from RMF guidelines will be documented with justification.

8. Conclusion

This Cybersecurity Policy is critical for protecting our manufacturing environment from cyber threats. All employees are responsible for adhering to this policy and reporting any suspected security incidents. By working together, we can ensure the confidentiality, integrity, and availability of our information and systems, and maintain business continuity. The CISO will have oversight of the policy and will review it on an annual basis, or more frequently as needed, based on changes in the risk landscape or business operations. The policy owner is responsible for ensuring the policy is effectively implemented and enforced.