Standard Operating Procedure (SOP) for Cybersecurity

For Boeing Parts Manufacturing Setup

1. Purpose

This SOP outlines cybersecurity protocols to protect sensitive data, intellectual property, and operational integrity in a Boeing parts manufacturing facility. It ensures compliance with industry standards, including **NIST SP 800-171**, **ISO 27001**, and **CMMC (Cybersecurity Maturity Model Certification)**.

---

2. Scope

Applies to all employees, contractors, and third-party vendors interacting with digital systems, networks, and industrial control systems (ICS) within the manufacturing setup.

---

3. Roles & Responsibilities

3.1 IT Security Team

- Implement and monitor cybersecurity policies.
- Conduct risk assessments and penetration testing.
- Ensure compliance with Boeing's cybersecurity requirements.

3.2 Manufacturing Personnel

- Adhere to cybersecurity best practices.
- Report any suspicious activity or security incidents.

3.3 Third-Party Vendors

- Follow **Boeing's cybersecurity guidelines**.
- Ensure secure data exchange using **encrypted channels**.

---

4. Access Control & Authentication

- Implement **role-based access control (RBAC)** with least privilege principles.
- Use **multi-factor authentication (MFA)** for all critical systems.

- **Disable inactive accounts** after 30 days of inactivity.
- Regularly audit and update access privileges.

---

5. Network Security Measures

- **Segregate networks** for IT, OT (Operational Technology), and third-party access.
- Use **firewalls and intrusion detection systems (IDS/IPS)** to monitor network traffic.
- Enable **VPN and end-to-end encryption** for remote access.
- Restrict USB and removable media usage to prevent unauthorized data transfer.

---

6. Data Protection & Encryption

- Classify and label data as **Confidential, Internal, or Public**.
- Use **AES-256 encryption** for sensitive Boeing-related data.
- Implement **secure file transfer protocols (SFTP, TLS 1.2+)** for data sharing.
- Enforce **automatic data backups** with offsite storage.

---

7. Industrial Control Systems (ICS) Security

- Isolate **ICS networks** from corporate IT infrastructure.
- Apply **patch management** for all ICS components.
- Restrict physical access to **SCADA and CNC machine control systems**.
- Monitor **IoT and IIoT (Industrial Internet of Things) devices** for anomalies.

---

8. Endpoint & Device Security

- Install **endpoint detection and response (EDR)** solutions.
- Enable **automatic OS and software updates**.
- Implement **application whitelisting** to prevent unauthorized software installation.
- Require **encrypted and company-approved devices** for accessing sensitive systems.

---

9. Incident Response Plan

9.1 Detection & Reporting

- Employees must report **phishing emails, unauthorized access, or malware infections** immediately.

- The IT team must **triage and analyze logs** from **SIEM (Security Information and Event Management) tools**.

9.2 Containment & Recovery

- Isolate affected systems **to prevent lateral movement**.
- Restore compromised data from **secure backups**.
- Conduct **post-incident forensic analysis** to identify root causes.

---

10. Security Awareness & Training

- Conduct **quarterly cybersecurity training** for employees.
- Perform **phishing simulations** and social engineering tests.
- Update employees on **new threats** and best practices.

---

11. Compliance & Audits

- Conduct **annual cybersecurity audits** based on **ISO 27001** and **CMMC Level 3** standards.
- Maintain **logs of all security events** for at least **12 months**.
- Ensure **third-party suppliers meet Boeing's cybersecurity requirements**.

---

12. Review & Continuous Improvement

- Review cybersecurity policies **annually**.
- Update protocols based on **threat intelligence reports**.
- Integrate **machine learning & AI-based anomaly detection** in security monitoring.

---

by: Irphan Salam
📅 *Effective Date: [Insert Date]*
🔄 *Next Review Date: [Insert Date]*