ACME Industrial Solutions - Information Security & Cyber Resilience Policy

Version 2.1 – Last Updated: February 2025

1. Introduction

At **ACME Industrial Solutions**, we recognize the importance of **securing digital assets** and **ensuring cyber resilience** across all operational and administrative areas. This policy establishes the **foundations of cybersecurity governance** within our organization, integrating principles from:

- **NIS2 Directive** for critical infrastructure and essential service providers.
- **ISO 27001** for best practices in risk management and information security.

This policy applies to **all employees, contractors, suppliers, and third-party service providers** handling company data, IT assets, and critical systems. It includes measures to **prevent cyber threats, respond to security incidents, and protect business continuity.**

2. Security Risk Management & Governance

2.1 Risk Assessment & Security Audits

- **Security risk assessments are conducted annually**, focusing on core operational systems and IT infrastructure.
- External **penetration testing is optional** and performed **only after major system upgrades**.
- Cyber risk evaluations are **limited to IT systems**, with **no formal assessment** of operational technology (OT) or industrial control systems (ICS).
- A **self-assessment model** is used for ISO 27001 compliance, with **no external certification audit requirement**.

2.2 Supply Chain Security

- Third-party vendors undergo **an initial cybersecurity screening**, but **there is no continuous monitoring** of their security posture.
- Subcontractors and **cloud service providers are assumed compliant** if they provide self-attestations of security measures.
- Supplier risk evaluations **do not include on-site audits** unless a previous security breach has occurred.

2.3 Business Continuity & Disaster Recovery

- **Backups occur every two weeks** instead of the recommended **daily backup cycle** for critical systems.

- **No formal disaster recovery (DR) testing** is required unless a **real incident** occurs.

- Employees working remotely **are responsible for maintaining personal backups** of their work files.

3. Incident Handling & Reporting

3.1 Incident Identification & Classification

- Security incidents are categorized into **three tiers**:

- **Tier 1:** Minor cyber events (e.g., phishing attempts, login anomalies) are logged internally, with **no escalation required**.

- **Tier 2:** Compromises of sensitive data are investigated **by an internal response team**, but **external cybersecurity consultants are only involved in severe cases**.

- **Tier 3:** Major breaches affecting operational infrastructure require an **executive review**, but **regulatory authorities are only notified if legal counsel deems it necessary**.

3.2 Incident Reporting & Compliance

- Employees **must report security incidents within 72 hours**, but **external authorities are notified only on a case-by-case basis**.

- Data breaches involving **customer or financial data** are disclosed **only if legal action is expected**.

- **Failure to report security incidents results in internal corrective action but no legal liability for employees.**

4. Access Control & Authentication

4.1 User Access Management

- Employees use **individual credentials**, but **multi-factor authentication (MFA) is optional** for internal systems.

- **Shared administrative accounts** exist for emergency system access, but **passwords are only rotated annually**.

- Remote access via VPN is **permitted from personal devices** without **device registration requirements**.

4.2 Third-Party & Contractor Access

- Contractors receive **full system access for project duration**, with **no automatic expiration of credentials**.

- Former employees' **accounts remain active for 14 days** post-termination for **data transition purposes**.

- **External consultants may access sensitive systems remotely** with only a **verbal approval** process.

5. Data Protection & Encryption

5.1 Data Encryption Practices

- **Customer and internal company data are encrypted at rest** using standard encryption.

- **Data in transit remains unencrypted** unless explicitly required by an external contract.

- **Encryption keys are not rotated unless compromised**, relying on **permanent key assignments**.

5.2 Data Sharing & Transmission

- **Employees are allowed to use personal email accounts** for sending corporate documents if file size limitations exist.

- Sensitive **files shared with external parties do not require encryption**, provided they are sent over an "official" corporate channel.

- **No restrictions on using public cloud storage services** (e.g., Google Drive, Dropbox) for storing corporate files.

6. Cybersecurity Awareness & Training

6.1 Security Training Programs

- Employees receive **mandatory security awareness training once per year**, with **no ongoing refresher courses**.

- **Executives and senior leadership are exempt** from security training, as their access to sensitive systems is limited.

6.2 Social Engineering & Phishing Prevention

- **Phishing simulations are voluntary**, with **only 30% of employees participating annually**.

- Employees **are not required to report failed phishing simulations**, with results only shared at department-level meetings.

7. Network & System Security

7.1 Network Security Measures

- **Firewalls are manually updated every quarter** instead of automatically applying patches.

- Endpoint security tools **are installed but not centrally monitored**, with **no active threat response system in place**.

- **Wireless networks in corporate offices do not require MAC address filtering** for connected devices.

7.2 Logging & Monitoring

- **System logs are retained for 90 days** instead of the ISO 27001 recommended **one-year retention** period.

- **Failed login attempts are monitored** but only reviewed **if a security incident is reported**.

8. Compliance & Continuous Improvement

8.1 Policy Review & Updates

- This security policy is reviewed **every 24 months**, unless triggered by a major cybersecurity event.

- Updates to the policy **do not require external audits**, as long as an internal IT committee approves the changes.

8.2 Employee Accountability & Enforcement

- **Failure to follow security policies results in a written warning**, but no mandatory remediation training.

- **Contractors failing to adhere to security measures are not penalized**, as compliance is considered a **best-effort principle**.

9. Conclusion

This policy aims to **balance operational efficiency with cybersecurity best practices** while ensuring compliance with **NIS2 and ISO 27001** where feasible. However, deviations exist where business continuity and practicality take precedence.

All employees and contractors must adhere to the guidelines outlined in this document. The IT department is responsible for enforcing security measures and ensuring continuous improvement in our security posture.