

SALZER ELECTRONICS LIMITED

INFORMATION SECURITY POLICY

Policy Statement

Salzer Electronics Ltd (SALZER) is committed to safeguarding the confidentiality, integrity, and availability of all information assets, including but not limited to customer data, business information, and IT infrastructure. To achieve this, SALZER has established a robust **Information Security Management System (ISMS)** that aligns with industry best practices, regulatory requirements, and organizational objectives.

Objectives & Commitments

To maintain and continually improve our **Information Security posture**, SALZER will:

1. **Risk Management & Threat Mitigation**
    - Proactively identify, assess, and mitigate security risks to protect information assets.
    - Implement strong controls and best practices to safeguard against cyber threats, data breaches, and unauthorized access.
2. **Compliance & Legal Adherence**
    - Ensure compliance with all applicable legal, statutory, and regulatory requirements related to information security.
    - Continuously monitor changes in laws and update policies accordingly.
3. **Security Awareness & Training**
    - Conduct regular **security awareness training** for all employees to instill a culture of security responsibility.
    - Encourage employees to recognize and report security incidents or potential threats.
4. **Incident Response & Business Continuity**
    - Establish a **structured incident response plan** to promptly detect, report, and mitigate security incidents.
    - Initiate corrective and preventive actions to avoid recurrence and minimize business impact.
    - Ensure business continuity through **disaster recovery planning** and resilience strategies.
5. **Access Control & Data Protection**
    - Enforce **role-based access control (RBAC)** and least privilege principles to restrict unauthorized access.
    - Protect sensitive data through **encryption, secure storage, and controlled sharing mechanisms**.
6. **Security Performance Monitoring & Continuous Improvement**
    - Regularly evaluate security controls through **audits, penetration testing, and vulnerability assessments**.
    - Review and enhance ISMS effectiveness through **management reviews and security performance metrics**.
    - Promote a culture of **continuous improvement and adaptability** in response to emerging security challenges.

Core Principles

SALZER's Information Security Policy is built upon the following three pillars:

Confidentiality: Protecting information from unauthorized access, disclosure, or misuse.
Integrity: Ensuring data accuracy, reliability, and protection from unauthorized modifications.
Availability: Guaranteeing access to information and services for authorized users when needed.

Responsibility & Compliance

- All employees, contractors, and third-party vendors must **adhere** to this policy and operate in compliance with the organization's security framework.
- Violations of this policy will be addressed through disciplinary measures and corrective actions.
- Leadership is committed to providing necessary resources and oversight to ensure effective implementation and continuous security enhancement.

END OF DOCUMENT