Information Security Management System at Blickfeld

Document revision 1.0, 17.02.2025

Revision history

Rev.	Date	Authors	Reviewed by	Approved by
1.0	17.02.2025 #55181	W. Rosenfeld	R. Wojtech	M. Müller

1. Introduction

1.1 Purpose of the ISMS

- Establish a structured framework for managing information security risks.
- Ensure the confidentiality, integrity, and availability of company assets.
- Support compliance with regulatory requirements and industry best practices.

1.2 Scope and Applicability

- Applies to all employees, contractors, and third-party service providers handling company information.
- Covers on-premise, remote work, cloud services, and third-party integrations.

1.3 Alignment with ISO 27001:2022

- Adopts principles of risk-based security management.
- Provides a foundation for the future ISO 27001 certification.

1.4 Key Objectives and Security Principles

- Establish clear security roles and responsibilities.
- Define access control mechanisms and authentication policies.
- Implement incident response and continuous security monitoring.

2. Governance and Responsibilities

2.1 Roles and Responsibilities

- **Management**: Fostering a culture of Cybersecurity awareness. Allocating resources, providing support for all related activities. Reviewing and approving policies, ensuring continuous improvement.
- **Project Managers**: Ensuring that security requirements are documented and integrated into project plans. Monitoring compliance with the security policy throughout the project lifecycle.
- **Chief Information Security Officer (CISO)**: Establishing and maintaining a Cybersecurity strategy tailored to the company size and needs. Overseeing policy development, inquiries and incident response.
- **Cybersecurity Team**: Developing Cybersecurity policies. Evaluating and implementing certifications and conformance.
- **Development Team**: Following secure coding practices throughout the SDLC. Participating in internal and external security training and awareness programs. Following CVE data feeds.
- **Testing Team**: Ensuring that the functionality fulfills specifications on all levels from unit to system. Identifying and reporting regressions and potential threats.
- **IT Team**: Maintaining IT infrastructure incl. user endpoint devices, installing and updating software. Implementing related policies.
- **Incident Response Team**: Leading and coordinating the incident response effort. Ensuring timely detection, reporting, and resolution of incidents.
- **Employees**: Adhering to all policies and reporting any security incidents or vulnerabilities.

2.2 Segregation of Duties

- Prevent conflicts of interest by separating critical functions (e.g., development, testing, deployment).
- Access rights must be distributed to reduce the risk of unauthorized actions.

3. Information Security in Project Management

3.1 Security Considerations in Project Planning

- Security requirements must be defined at the start of any project.
- Risk assessments must be conducted before project approval.

3.2 Security Controls During Development

- Use secure coding practices and follow security guidelines, detailed in the document **“Cyber Security Guideline for Software & System Development”**.
- Conduct periodic security review.

3.3 Post-Implementation Security Review

- Security assessment before project deployment.
- Implementation of monitoring and access control measures.

4. Access Control and Identity Management

4.1 Rules for Physical and Logical Access

- Access to physical premises and IT systems is granted based on job roles.
- Visitors must be accompanied by authorized personnel.

4.2 Handling of Authentication Information

- Use of strong password policies (length, complexity, expiration, enforcement of changing the initial password).
- Authentication information shall be communicated only after ensuring the recipient's identity.
- No sharing of credentials under any circumstances.

4.3 Access Control Policy

- Role-Based Access Control ensures least-privilege access, only providing access to the assets necessary for the fulfillment of specific duties.
- Periodic review of access rights to remove unnecessary privileges, e.g. when the roles change.

4.4 Identity Management

- Unique user IDs for all employees and contractors.
- No duplicate identities.
- Onboarding and offboarding processes ensure proper account provisioning and removal.

4.5 Access Rights Management

- Documented approval process for privileged access.
- Logging and monitoring of privileged accounts.
- Onboarding and offboarding processes ensure proper granting and revocation of access rights.
- Review of access rights according to the Access Control Policy defined above.

5. Information Security for Use of Cloud Services

5.1 Cloud Service Selection and Risk Management

- Cloud providers must comply with security and data protection regulations, in particular the ISO 27001 standard.
- Contracts should define security responsibilities (shared responsibility model).

5.2 Access and Authentication in Cloud Environments

- Use of SSO for cloud-based applications where possible.
- Implementation of Zero Trust Architecture (ZTA) principles where possible.

5.3 Data Protection in Cloud Services

- Encrypted transfer of sensitive data to and from the Cloud Service.
- Encryption of sensitive data before uploading where possible.
- Regular security assessments of cloud configurations.

6. Information Security Event Reporting and Incident Handling

6.1 Incident Management

- A dedicated Incident Response Team (IRT) is responsible for overseeing all stages of an incident: detection, assessment and resolution.
- Detailed policy is documented in "**Incident Response Policies and Procedures**".

6.2 Incident Reporting Guidelines

- Employees must report all security incidents (e.g. phishing, malware infections).

6.3 Communication and Escalation

- Significant incidents must be escalated to management.
- Communication to customers, partners and contractors where needed in compliance with legal and contractual obligations.

7. Documented Operating Procedures

7.1 Security Policy Documentation

- Policies must be documented, approved, and reviewed annually.
- Employees must acknowledge and comply with security policies.

7.2 Policies concerning Cybersecurity

- "**General Measures**": summarizes all basic aspects and measures.
- "**Security Guideline for Software & System Development**": outlines measures specific to development of SW and products.

8. Compliance and Continuous Improvement

8.1 Policy Review and Updates

- Regular updates to reflect emerging threats and compliance changes.
- Employees must be informed of any policy updates.

8.2 Auditing and Monitoring

- Periodic internal audits to ensure policy compliance conducted by the Cybersecurity Team.

8.3 Continuous Improvement

- Security incidents are analyzed to improve security measures.
- Adoption of new technologies and best practices.