QM-4-IT /
LOGO

Title:

Information Security Policy

Document Information

Document ID	SEC-POL01
Version	1.0
Status	Effective
Category	Policy
Creation Date	01-Jan-2026
Issue Date	01-Jan-2026
Effective Date	01-Jan-2026
Supersedes Document	N/A
Disclaimer	This document contains confidential information. Do not distribute this document without prior approval from higher management of **QM-4-IT**

Role	Name	Title	Date	Signature
Author(s)	Alfred Schlaegel	CEO		
Reviewer(s)	John Doe	CEO		
Approver(s)	Jane Doe	QA		

Table of Content

1 PURPOSE

The purpose of this Information Security Policy is to establish and maintain the security and confidentiality of information, integrity of business operations, and protection of all physical and intellectual assets of the company.

2 SCOPE

This policy applies to all employees, contractors, consultants, temporary workers, and other workers at the company, including all personnel affiliated with third parties.

3 REFERENCES

3.1 Internal References

- Document: QA-IR01 Internal References

3.2 External References

The company has shaped its Information Security framework around the fundamental principles of the following internationally recognized standards or regulations:

- ISO 27001:2022 - Information Security Management Systems - Requirements
- ISO 27031:2011 - Guidelines for Information and Communication Technology Readiness for Business Continuity
- ISO/IEC 27017:2022 - Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services
- NIST SP 800-40 - Guide to Enterprise Patch Management Technologies
- NIST SP 800-57 - Recommendation for Key Management

4 ABBREVIATIONS, TERMS & DEFINITIONS

Term	Definition
GDPR	General Data Protection Regulation
HIPAA	The Health Insurance Portability and Accountability Act

5 ROLES AND RESPONSIBILITIES

Role	Responsibilities
Management	Ensure that an appropriate Information Security Management System (ISMS) is established, implemented, and maintained.
Employees	Comply with the Information Security Policy and related procedures.

Information Security Officer	Oversee the ISMS, coordinate audits, and manage security incidents. Represented by Security Department.

6 PROCEDURE

6.1 Information Security Framework and Governance

Company Name will establish and maintain a robust Information Security framework and overseeing the Information Security governance framework. This includes:

- identifying and classifying information assets
- defining security roles and responsibilities
- implementing security controls
- monitoring the effectiveness of these controls

and ensuring that all Information Security practices align with the company's objectives and risk appetite.

6.2 Policy, Procedure, Guidelines, and Compliance

Company Name will develop and maintain clear Information Security policies, procedures, and guidelines, which are regularly reviewed and updated to reflect changes in the threat landscape, business objectives, and regulatory requirements.

6.3 Human Resources and Information Security Training

Company Name will ensures that Information Security considerations are integrated into all HR activities and that all employees receive regular Information Security training including security responsibilities in job descriptions and employment contracts. HR will also conduct proper security checks, including background checks, for all new hires.

6.4 Asset and Data Life Cycle Management

Company Name will ensure that all assets, including information, software, hardware, and data, are identified, classified, and managed throughout their life cycle. This includes maintaining an up-to-date asset inventory, implementing appropriate security controls for each asset, securely disposing of assets when they are no longer needed, and managing data from creation and storage to disposal.

6.5 Information Security in Software Development and Network Management

Company Name will ensure that security is integrated into all stages of the software development lifecycle and the company's network infrastructure. This includes conducting threat modeling during the design phase, implementing secure coding practices during the development phase, performing security testing before deployment, designing a secure network architecture, implementing security controls such as firewalls and intrusion detection

systems, monitoring network traffic for suspicious activity, and updating network equipment to patch vulnerabilities.

6.6 Physical, Logical, and Web Security

Company Name will ensure the physical and logical security of the company's assets and web, gateway, and endpoint security measures. This includes implementing physical security controls such as access controls and CCTV, and logical security controls such as firewalls, intrusion detection systems, antivirus software, web application firewalls, secure gateways, and endpoint protection solutions.

6.7 Infrastructure Management

Company Name will ensure that data are protected throughout their life cycle and the security of the company's infrastructure. This includes implementing security controls such as spam filters and phishing filters, encrypting sensitive emails, educating users on safe email practices, selecting secure service providers, implementing security controls in the environment, and monitoring the environment for security incidents.

6.8 Vulnerability, Patch Management, and Backup and Restore

Company Name will establish responsibilities for the company's vulnerability and patch management process and ensures that regular backups of critical data are taken and stored securely. This includes conducting regular vulnerability scans, assessing the risk of identified vulnerabilities, applying patches in a timely manner, verifying the success of patch installations, defining the backup schedule and methods, testing backups to ensure they can be restored, and implementing a disaster recovery plan to restore operations in the event of a data loss incident.

6.9 Incident Management and Information Security Resilience

Company Name will establish an incident management process and ensures that the company is prepared to continue operations in the event of a security incident. This includes defining the incident response plan, coordinating the response to Information Security incidents, conducting post-incident reviews to identify lessons learned, updating the incident response plan based on these lessons, developing a business continuity plan, testing the plan to ensure it is effective, and updating the plan based on test results and changes in the business environment.

6.10 Third-party Requirements, Risk Management, and Audit Management

Company Name will establish a process to ensure that third parties and suppliers comply with the company's Information Security policy, manage the Information Security risk life cycle, and coordinate regular Information Security audits. This includes including security requirements in contracts, conducting security assessments of third parties, monitoring third-party compliance, identifying potential risks, conducting risk assessments to determine their impact and likelihood, implementing measures to mitigate high-risk threats, monitoring the effectiveness of these measures, defining the audit scope and schedule, selecting auditors, reviewing audit results, and implementing necessary changes based on audit findings.

7 ATTACHMENTS

ID	Name	Description
ATT01	Information Security Framework Diagram	A visual representation of the Information Security framework, including the classification of information assets, security roles and responsibilities, and security controls.

8 DOCUMENT REVISION HISTORY

Author(s)	Date	Version	Description
Alfred Schlaegel	01-Jan-2025	1.0	Initial Version