

Policy for

Information Security

Table of content

Introduction	2
Scope	2
Policy Statements	3
Management Approval	5
Objectives, Review and Maintenance	5

Introduction

At itm8, our unwavering commitment to information security is guided by the vision set forth by our Top Management. As a leading organization in our industry, we recognize that the effective protection of information assets is paramount to our success.

This Information Security Policy serves as the cornerstone of our dedication to maintaining the highest standards of information security to ensure itm8 continues to be considered a trustworthy partner for both national and international customers and stakeholders.

Our vision is to establish an environment where Information Security is not just a requirement, but a fundamental value that underpins every aspect of our operations and organization.

Scope

This policy is applicable to all employees, contractors, partners, and third parties engaged with itm8. This includes all itm8 companies and locations, as well as entities with access to our information assets and resources. The policy covers all forms of information, whether digital or physical, and extends to all systems, networks, devices, and facilities utilized within our organization.

Information Security in itm8 is defined as the practice of protecting and mitigating threats to information processing facilities to uphold data confidentiality, integrity, and availability. itm8 implements all requisite activities to ensure:

- **Confidentiality:** To establish the possibility for confidential handling, transmission and storage of data to which only authorized and authenticated users have access.
- **Integrity:** To achieve proper functioning of systems with a minimal risk of manipulation, data loss and errors in both data and systems.
- **Availability:** To achieve a high degree of availability with high up-times and a minimal risk of major breakdowns.

This Information Security Policy is governing the entirety of itm8, which means that all customer divisions, business divisions, and employees in any of them, is subject to this policy.

Policy Statements

As a leading IT service provider, itm8 is committed to ensuring high standards of information security, sustainability, and regulatory compliance. This policy, endorsed by our Top Management, reflects our dedication to protecting the integrity, confidentiality, and availability of information across all our operations.

UNIFORM INFORMATION SECURITY MANAGEMENT

itm8 is dedicated to meticulous development, implementation and continuous improvement of a uniform Information Security Management System (ISMS) aligned with our business strategy. Our ISMS adheres to ISO/IEC 27001:2022, ISO/IEC 27701, NIS2, GDPR, and sustainability goals, ensuring consistent security practices across all service areas.

CLEARLY DEFINED ROLES AND RESPONSIBILITIES

itm8 defines and assigns clear roles and responsibilities for information security throughout the organization. itm8 strives to ensure that all employees and partners understand their obligations, fostering a culture of accountability and proactive security.

RIGOROUS AUDITS AND ASSESSMENTS

itm8 is committed to conducting regular and thorough audits and assessments, maintaining compliance with ISO/IEC 27001:2022 and all applicable regulatory and statutory requirements. These evaluations will be integral to verifying the effectiveness and consistency of our security.

CONSISTENT RISK MANAGEMENT

itm8 employs a standardized risk management framework to identify, assess, and mitigate security risks across the organization. This approach minimizes vulnerabilities and reduces the likelihood of security incidents, ensuring uniformity in our risk management efforts.

DATA PROTECTION AND COMPLIANCE

itm8 is committed to the comprehensive protection of all entrusted data, including intellectual property, confidential business information, and personal identifiable information (PII). We implement advanced and consistent security measures across all platforms and services to guard against unauthorized access, breaches, and other threats, in full compliance with GDPR, NIS2 and other relevant regulations.

RESOURCE ALLOCATION FOR SECURITY INITIATIVES

itm8 ensures adequate resources will be allocated to support the effective implementation of our Information Security Policy and initiatives. This ensures that our security objectives are met comprehensively and sustainably across the organization.

EXECUTIVE OVERSIGHT

itm8 places the ultimate accountability for information security at the Top Management level, ensuring strong leadership and alignment with organizational goals. This oversight will guarantee that our Information Security Function operates effectively and consistently.

FOSTERING A SECURITY-CONSCIOUS CULTURE

itm8 promotes a culture of security awareness throughout our organization, encouraging employees and partners to actively contribute to information protection. Continuous education and critical thinking will be key to upholding our security standards uniformly.

STANDARDIZED GOVERNANCE AND INCIDENT RESPONSE

itm8 maintains a standardized governance structure for information security across all operations. This consistent approach will extend to our incident response procedures, ensuring that security incidents are managed swiftly and effectively and in accordance with contractual and regulatory requirements.

SUPPLIER SECURITY MANAGEMENT

itm8 enforces and assesses high security standards among our suppliers and third-party partners, requiring them to adhere to the same stringent protocols we uphold internally. This ensures a secure and consistent approach to information across our supply chain.

INTEGRATED SECURITY AND PRIVACY FRAMEWORK

itm8 utilizes a standardized framework for the management system, which is both our ISMS and Privacy Information Management System (PIMS), ensuring that our security and privacy practices are comprehensive, consistent, and aligned with best practices and sustainability objectives.

INDEPENDENT EXTERNAL ASSURANCE AUDITING

itm8 engages in external independent assurance audits, where applicable, to obtain an objective evaluation of our information security initiatives. This process ensures that our security practices are accurately validated and reflect a trustworthy assessment of our commitment to information security.

COMPLIANCE, ENFORCEMENT AND INCIDENT REPORTING

itm8 requires all employees, contractors, and partners to comply with this policy and its supporting policies and procedures. All personnel are required to report actual or suspected security incidents and weaknesses without undue delay through the established channels. Breaches of this policy may lead to disciplinary or contractual consequences in accordance with applicable law and agreements.

This policy reflects itm8's commitment to a consistent and unified approach to information security, ensuring that practices are aligned with our business strategy, regulatory requirements, and sustainability objectives.

Management Approval

The itm8 executive management team fully endorses and commits to the statements outlined in this Information Security Policy. We provide the necessary resources, support, and oversight to ensure the continuous improvement and effectiveness of our Management System.

By approving this document, we affirm our unwavering commitment to maintaining the highest standards of information security, regulatory compliance, and sustainability across all itm8's operations.

This Information Security Policy serves as a cornerstone of our strategic approach to safeguarding the confidentiality, integrity, and availability of all information assets under our management.

Objectives, Review and Maintenance

This policy provides the framework for setting and reviewing itm8's information security objectives and their achievement. The policy is reviewed at least annually, and whenever significant changes occur, to ensure its continued suitability, adequacy, and effectiveness. It is communicated to all employees and made available to relevant interested parties, such as customers and partners, as appropriate.

Policy approved by itm8 management on 19 August 2026.