ITML Quality and Information Security Policy

info@itml.gr

+30 211 800 1862

16 November 2024

Revisions

Date	New Version	Reason
16/11/2024	2	ISO 27001:2022 transition

Table of Contents

1. Purpose & Scope 4
2. Leadership Commitment & Management System Integration 4
3. Quality Management Policy 5
4. Information Security Policy 6
5. Roles & Responsibilities 6
6. Compliance & Continuous Improvement 7
7. Policy Approval & Review 7

1. Purpose & Scope

This policy outlines ITML's commitment to Quality Management & Information Security. It applies to all employees, contractors, partners, and stakeholders who interact with ITML's systems, products, and services. ITML ensures adherence to ISO 9001:2015 (Quality Management) and ISO 27001:2022 (Information Security), along with compliance with GDPR and other applicable regulatory frameworks.

2. Leadership Commitment & Management System Integration

ITML's top management is fully committed to the effective implementation and continual improvement of both the Quality Management System (QMS) and the Information Security Management System (ISMS).

The Top Management of ITML commits to:

- Assume responsibility for the effectiveness of the Quality and Information Security Management System.
- Establish and communicate the Information Security and Quality Policy and related objectives, aligning them with ITML's strategic direction.
- Integrate management system requirements into the organization's operational processes.
- Promote the use of the process approach and risk-based thinking.
- Ensure the availability of resources necessary for the Management System.
- Emphasize the importance of effective quality and information security management, and compliance with applicable requirements.
- Encourage continuous improvement across all organizational levels.
- Support and engage personnel at all levels to contribute to the effectiveness of the system.

- Promote continual improvement and support other management roles to demonstrate leadership in their areas.

3. Quality Management Policy

ITML is committed to delivering high-quality, innovative, and user-focused IT solutions by:

- Maintaining a customer-centric approach to software development, IT consulting, and cybersecurity services.
- Continuously improving processes, tools, and methodologies to enhance efficiency and effectiveness.
- Complying with all relevant industry standards and best practices.
- Encouraging a culture of innovation, agility, and continuous learning.
- Monitoring and evaluating performance through regular audits, feedback mechanisms, and KPIs.

ITML's quality objectives include:

- Achieving **99% client satisfaction rate** in delivery service.
- Reducing defect rates in software products to **below 1%**.
- Ensuring that **100% of employees undergo quality and compliance training annually**.

4. Information Security Policy

ITML recognizes the importance of protecting information assets and ensuring the confidentiality, integrity, and availability (CIA) of data. ITML is committed to:

- Implementing and maintaining an **ISO/ IEC 27001-compliant Information Security Management System (ISMS)**.
- Ensuring that all data processing activities comply with **GDPR and relevant cybersecurity and information security regulations**.
- Protecting ITML and client assets from cyber threats, unauthorized access, and data breaches.
- Conducting **periodic security assessments, penetration testing, and risk evaluations**.
- Enforcing strict **access controls, authentication mechanisms, and encryption** for sensitive data.

ITML's information security objectives include, but are not limited to:

- Ensuring **100%** of employees complete cybersecurity awareness training annually.
- Maintaining **zero tolerance** for critical security incidents.
- Applying multi-factor authentication (MFA) and encryption across all sensitive systems and data.
- Conducting regular risk assessments, penetration tests, and reviews of technical and organizational controls.

5. Roles & Responsibilities

- **Executive Management**: Ensures that quality, security, and privacy policies are enforced and aligned with business goals.

- **IT & Security Team**: Manages security controls, risk assessments, and compliance with ISO/IEC 27001 and GDPR.
- **Employees & Contractors**: Adhere to all security, privacy, and quality guidelines in daily operations.
- **Clients & Partners**: Expected to comply with ITML's security and privacy requirements when accessing systems and data.

6. Compliance & Continuous Improvement

- Regular internal and external audits will be conducted to ensure compliance with ISO 9001, ISO/IEC 27001, GDPR, and other applicable laws.
- ITML will provide ongoing training to employees on quality management, cybersecurity best practices, and data privacy laws.
- Policies and procedures will be reviewed **annually** to reflect evolving industry standards and regulatory requirements.

7. Policy Approval & Review

This policy is reviewed annually and updated as necessary to align with new legal and technological developments.