ERIKLABS

Integrated Quality and Information Security Policy

ISO 9001:2015 Clause 5.2 and ISO/IEC 27001:2022 Clause 5.2

Document Code	Review	Publication Date	Security
PL-01	00	31.07.2026	Publicly Available

Preparer	Controlled by	Approved
Quality and ISMS Manager	Software Development Manager	General manager

The aim of the policy: The aim is to define common directions and commitments for ErikLabs to manage its software development and software testing services in accordance with the principles of customer satisfaction, reliable service, information security, risk management, and continuous improvement.

1. Policy Statement

ErikLabs aims to provide its customers with reliable, verifiable, secure, and sustainable products and services in software development, software testing services, technical maintenance, and related support processes. It establishes, implements, maintains, and continuously improves its Quality Management System and Information Security Management System in accordance with the organization's purpose, strategic direction, the nature of its activities, and its risks.

Through this policy, senior management makes the following commitments:

- Accurately understanding customer needs, contract and acceptance criteria; meeting applicable requirements and continuously improving customer satisfaction.
- To conduct software development and testing services offered to clients using planned, traceable, unbiased, repeatable, and evidence-based methods.

- Ensuring product and service quality through requirements management, secure design, code review, testing, verification, validation, controlled release, and post-service monitoring.
- To protect the confidentiality, integrity, and accessibility of information; and to manage the risks of unauthorized access, alteration, disclosure, loss, and service interruption through appropriate controls.
- To classify and protect entrusted information assets, including customer source code, test environment, test data, findings, and reports, for the limited purpose.
- Systematically assessing information security and quality risks; mitigating unacceptable risks and seizing opportunities.
- Comply with applicable legal, regulatory, contractual, customer, and other relevant party requirements.
- To provide a measurable framework for setting, monitoring, and reviewing quality and information security objectives.
- To improve the competence, awareness, sense of responsibility, and safe work practices of employees and related external resources.
- Learning from incidents, errors, nonconformities, customer feedback, audits, and performance results; eliminating the causes and preventing recurrence.
- To continuously improve the suitability, adequacy, and effectiveness of the Quality Management System and the Information Security Management System.
- To provide the human, technological, infrastructure, time, and financial resources necessary for the implementation of these policies and systems.

2. ErikLabs Quality Principles

- Customer focus: Needs, intended use, acceptance criteria, and feedback are inputs for product and service decisions.
- Process approach: Development planning and scope, technical design, coding, code review, testing/deployment, maintenance, and technical improvement processes are managed with measurable outputs.
- Evidence-based decision-making: Test results, failure trends, KPIs, customer satisfaction, delivery performance, and audit results form the basis of decisions.
- Defect prevention: Instead of only catching errors at the final inspection, it is essential to prevent them through risk-based planning, review, automation, and early testing.
- Service reliability: The scope, methodology, environment, version, evidence, and report integrity of the testing services provided to customers are maintained; false positive/negative findings are minimized.
- Continuous improvement: Performance targets, root cause analyses, lessons learned, technical debt, and improvement opportunities are addressed regularly.

3. ErikLabs Information Security Principles

- Access is granted on a minimum privilege and need-to-know principle basis; authentication, authorization, and access logs are implemented.
- Development, testing, and production environments are separated; production data is not used in testing by default, and masking/anonymization and authorized approval are applied when necessary.
- Source code, configuration, secrets, dependencies, and software packages are protected within a secure development lifecycle.
- Information assets are classified; storage, transfer, backup, destruction, and restoration controls are applied in proportion to the risk.
- Information security incidents and vulnerabilities are reported promptly, recorded, addressed, and lessons are learned from the incidents.
- Suppliers, cloud services, and outsourcing are selected and monitored according to information security, confidentiality, continuity, and terms of service.
- Backup, monitoring, capacity, incident response, and recovery capabilities are maintained to ensure business continuity and technical resilience.

4. Framework for Quality and Information Security Objectives

Objectives are planned in accordance with this policy, are measurable, and have a defined responsibility and timeframe. Customer and stakeholder expectations, risks and opportunities, process performance, legal/contractual requirements, technological changes, and resources are considered when developing objectives. Objectives and indicators are defined in at least the following areas:

Target area	Sample monitoring indicators
Customer and service quality	Customer satisfaction, on-time delivery, initial acceptance rate, test report initial acceptance rate.
Software quality	Production failure, initial test pass, re-opened failure, code review compliance.
Information security	Incident rate/impact, vulnerability patching time, access review, awareness outcomes.
Service continuity	Availability, backup success, restore/rollback time, change success rate.
Competence and improvement	Competency development, corrective action effectiveness, recurring nonconformity, improvement actions.

The results of the objectives are monitored at the specified intervals. When an objective is not achieved, the deviation, cause, impact, correction/corrective action, responsible party, and deadline are recorded; the results are submitted to management for review.

5. Roles and Responsibilities

The policy is owned by senior management. Senior management ensures that the policy is aligned with the organization's context and strategic direction, integrated into systems, and that the necessary resources are provided. All employees and stakeholders working on behalf of ErikLabs are responsible for complying with this policy, procedures related to their duties, and safety/quality requirements communicated to them.

- The Quality and ISMS Officer coordinates the documentation, publication, awareness, performance, and review of the policy.
- Process owners implement policy commitments through process objectives, controls, records, and improvement activities.
- Employees uphold customer requirements, report errors/non-conformities and information security incidents, and do not perform actions outside their authorization.
- Suppliers and external sources comply with the quality, confidentiality, security, and reporting requirements specified in the contracts.

6. Communication, Understanding, and Accessibility

The policy is kept up-to-date as documented information. It is communicated within the organization through onboarding/orientation, periodic awareness training, meetings, internal communication channels, and the document management system. Employee understanding of the policy is verified through training participation, brief assessments, interviews, internal audits, and implementation observations.

The policy is made available to customers, suppliers, business partners, public institutions and other interested parties via the website, offer/contract addendum or controlled sharing channel where appropriate. Trade secrets or security-sensitive practice details are not included in the publicly available policy text.

7. Review and Update

The policy is reviewed at least once a year as part of a Management Review; it is also reviewed whenever there are changes in the organization's purpose, strategic direction, scope, stakeholder needs, legislation, technology, risk profile, customer requirements, or significant events. The review assesses the policy's appropriateness, adequacy, effectiveness, level of understanding, and alignment with objectives. Changes are approved

by senior management, the revision is published in a controlled manner, and communicated to relevant stakeholders.

Appendix A – ISO 9001 and ISO/IEC 27001 Clause 5.2 Compliance Matrix

Necessity	Its equivalent in politics	Application/proof
Suitability to the organization's purpose and context.	Policy Statement; ErikLabs' activities and strategic direction	Context analysis, scope, YGG record
Framework for quality objectives	Chapter 4 – Framework for Quality and Information Security Objectives	Target plan, KPI results, actions.
Information security objectives or a framework for setting objectives.	Chapters 3 and 4	ISMS objectives, risk treatment and monitoring records.
Commitment to meeting applicable conditions	Customer, legal, contractual and related party commitments in the Policy Statement	Regulations/requirements list, contract review.
Continuous improvement of the QMS	Quality Principles and Policy Commitments	DÖF, KPI, internal audit, YGG
Continuous improvement of the ISMS	Information Security Principles and Policy Commitments	Risk, incident, audit, DÖF and YGG.
Available as documented information.	Chapter 6	Approved policy, revision history.
Communication, understanding, and implementation within the organization.	Chapter 6	Training/awareness, interviews, internal audits.
Presented to the relevant parties in an appropriate manner.	Chapter 6	Website, offer/contract addendum, controlled sharing.