tinQwise

Version 2025.02

TinQwise Policy

014.0

System Acquisition, Development & Maintenance Policy

tinQwise

Validity and document management

Version	Date	Author	Description
01	2023-11-02	Emil de Valk	Document creation
02	2024-12-12	Emil de Valk	Annual Review & policy update

This document is valid as of January 1st, 2025.

The owner of this document are the C.O.O and H.o.E., who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- (Number of) incidents arising from failed security controls built into the systems
- Feedback from third party security advisors during the bi-annual security reviews
- Security findings from third party security assessments, white box penetration testing and code reviews
- Client IT organisation feedback & requirements

TinQwise reserves the right to update this Policy to reflect changes in our practices and regulatory requirements. Data subjects will be informed of material changes. Previous versions of this procedure will be stored for a period of 5 years, unless specified otherwise by legal or contractual requirement.

tinQwise

Table of Contents

tinQwise

1. Relevant to

Management	Finance / Legal	HR	Office Management	Marketing, Sales and Account Management	Professional services	IT Support	Product & Engineering	DevOps	Support & Maintenance
X						X	X	X	X

2. Purpose

This policy outlines the principles, guidelines, and best practices for the acquisition, development, and maintenance of information systems within TinQwise to ensure information security and compliance with ISO 27001 Annex A.14.

3. SCOPE

This policy applies to all information systems, software applications, and technology solutions developed, acquired, or maintained by TinQwise that process, store, or transmit sensitive information, including but not limited to Personal Data and intellectual property.

4. POLICY STATEMENTS

4.1 Acquisition of Information Systems

- TinQwise performs a risk assessment before acquiring any information system. This assessment will consider potential security risks, compliance requirements, and the impact on the confidentiality, integrity, and availability of information.
- Vendors and suppliers providing information systems must adhere to TinQwise information security requirements. Contracts and service level agreements must include security clauses, outlining responsibilities and security standards.
- Prior to acquisition, information systems will be evaluated and tested for security vulnerabilities and compliance with TinQwise information security policies and ISO 27001.

4.2 Development of Information Systems

- TinQwise implements a secure software development policy that includes security requirements, code reviews, and security testing.
- Developers and development teams receive regular training in secure coding practices and must be aware of common software vulnerabilities.

- Security assessments and code reviews are conducted before launching new software applications or major updates.
- Secure coding practices, such as input validation and access controls, are implemented to prevent common vulnerabilities like SQL injection, cross-site scripting (XSS), and authentication flaws.

4.3 Maintenance of Information Systems

- Regular patch management processes are established to promptly address and apply security updates and fixes to software and systems.
- Change management procedures are in place to ensure that changes to systems, software, and configurations do not introduce vulnerabilities.
- Retired information systems are securely decommissioned, and sensitive data properly disposed of in compliance with applicable regulations.

4.4 Compliance and Monitoring

- The Data Protection Officer (DPO) and the Security Committee are responsible for monitoring compliance with this policy.
- Regular audits and assessments are conducted to ensure compliance with ISO 27001 Annex A.14 and TinQwise information security policies.
- Non-compliance or security incidents must be promptly reported and addressed through TinQwise incident response and corrective action processes.

5. Communication

All employees, contractors, and relevant stakeholders must be made aware of and trained on this policy.

6. IMPLEMENTATION

This policy is effective immediately and is incorporated into TinQwise information security and risk management system (ISRMS).

7. COMPLIANCE TO THIS POLICY

The C.O.O. is responsible for verifying compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits. Any exception to the policy is subject to the Information security exceptions management process.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

tinQwise

8. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Evaluation of used third-party libraries and components and Security report	SharePoint	C.O.O.	Only team members can access these files	2 years
Procedures for secure information system engineering and secure development lifecycle	SharePoint and / or GitLab	C.O.O.	Only team members can access these files	2 years
Pentest and other security test reports	SharePoint	C.O.O.	Only team members can access these files	2 years