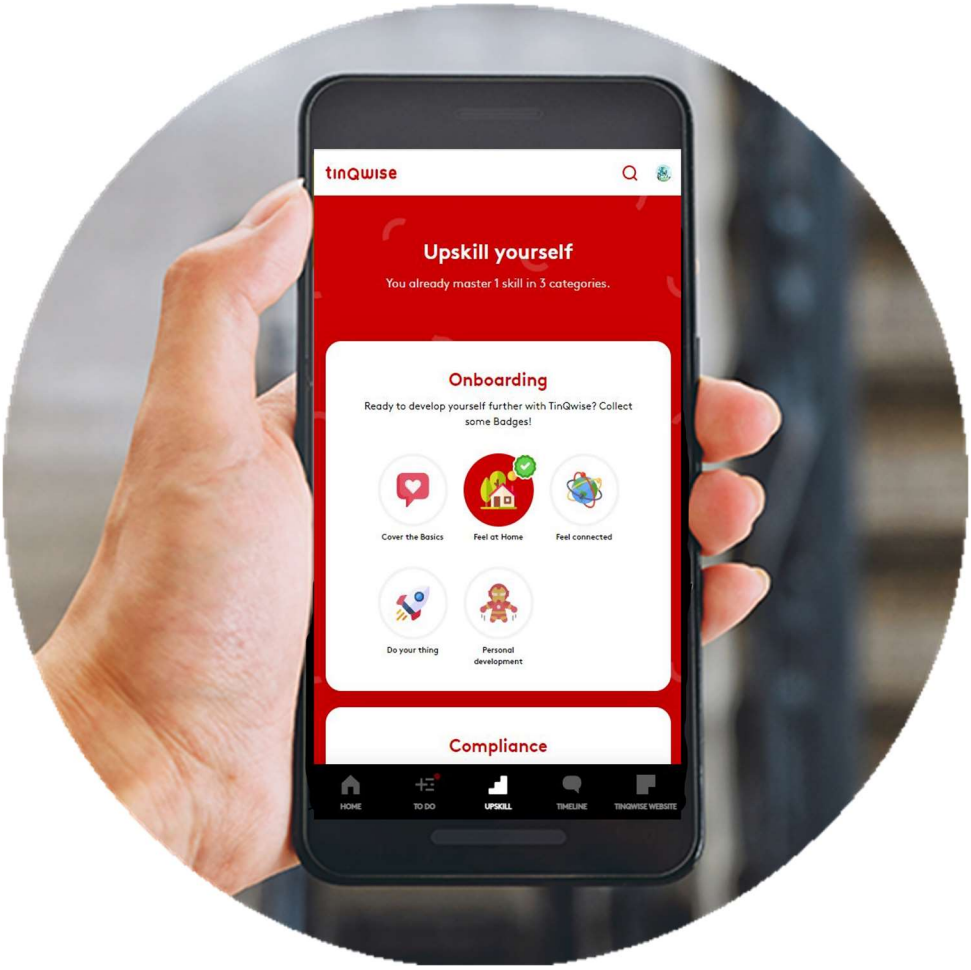
Version 2024.06

TinQwise Policy



003.3 Secure Development

tinQwise

VALIDITY AND DOCUMENT MANAGEMENT

Version	Date	Author	Description
01	2020-02-14	Simon Kennedy	Document creation
02	2020-12-12	Simon Kennedy	Annual review and policy update. Major updates based on organisation changes and updated procedures
03	2021-10-28	Simon Kennedy and Emil de Valk	Annual review and policy update.
04	2022-11-04	Simon Kennedy, Emil de Valk, Okke Formsma and Elena Neagu	Annual review and policy update
05	2023-03-09	Emil de Valk and Reinoud van Dommelen	Update to align with standard customer contract set. Definitions, renumbering and consistency.
06	2023-11-02	Okke Formsma and Emil de Valk	Annual review & update security requirements and release naming conventions.

This document is valid as of December 1, 2023.

The owner of this document are the C.T.O and the Head of Engineering, 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 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

VALIDITY AND DOCUMENT MANAGEMENT ---- 2

TABLE OF CONTENTS ---- 3

1. RELEVANT TO ---- 4

2. PURPOSE ---- 4

3. SCOPE ---- 4

4. REFERENCE DOCUMENTS ---- 4

5. SECURE DEVELOPMENT AND MAINTENANCE ---- 5

5.1 Risk assessment for the development process ---- 5
5.2 Securing the development environment ---- 5
5.3 Secure engineering principles ---- 5
5.4 Security requirements ---- 5
5.5 Checking and testing the implementation of security requirements ---- 5
5.6 Repository ---- 6
5.7 Version control ---- 6
5.8 Change control ---- 6
5.9 Protection of test data ---- 6
5.10 Required Security Training ---- 6
5.11 Information about secure development procedures and practices for customers ---- 6

6. COMPLIANCE TO THIS POLICY ---- 6

7. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT ---- 7

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

The purpose of this document is to define rules for secure development of TinQwise Platform software and systems. In general, all developers must adhere to the O.W.A.S.P. Secure Coding Practices, and follow O.W.A.S.P. guidelines in terms of a secure software development lifecycle and secure coding standards.

The goal of software security at TinQwise is to maintain the confidentiality, integrity, and availability of information resources. This goal is accomplished at TinQwise through the implementation of our Information Security & Risk Management System (ISRMS) and security controls.

3. SCOPE

This document focuses on the technical controls specific to mitigating the occurrence of common software vulnerabilities in the development and maintenance of our services, architecture, software and systems. The primary focus is on TinQwise Platform web applications and their supporting infrastructure.

4. REFERENCE DOCUMENTS

- O.W.A.S.P. Secure Coding Practices Quick Reference Guide (https://owasp.org/)
- ISO/IEC 27001 standard, clauses A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1
- ISO/IEC 27017 standard, clauses 14.2.1 and 14.2.9
- ISO/IEC 27018 standard, clause A.9.2
- 002.1 TinQwise ISRMS Governance
- 003.3 TinQwise Security Incident Management Policy
- 003.4 TinQwise Change Management Policy

tinQwise

5. SECURE DEVELOPMENT AND MAINTENANCE

5.1 RISK ASSESSMENT FOR THE DEVELOPMENT PROCESS

In addition to the risk assessment the C.T.O. & Head of Engineering periodically perform an assessment of the following:

- risks related to unauthorized access to the development environment;
- risks related to unauthorized changes to the development environment;
- technical vulnerabilities of the IT systems used in the organization, and specifically the development and engineering pipeline;
- the risks a new technology brings if used in the organization;
- risks related to secure development practices and code review.

5.2 SECURING THE DEVELOPMENT ENVIRONMENT

The development and production environments are separated by using separate Kubernetes environments and are accessible only through VPN. As they are built on templates, their security is ensured by using the same tools and policies, as described in the System Architecture, part of the Operational Resilience & Disaster Recovery policy. Access to the development environment is documented in the Access Control Policy.

5.3 SECURE ENGINEERING PRINCIPLES

The Head of Engineering and the C.T.O. will issue procedures following OWASP guidelines for secure information system engineering, both for the development of new systems and for the maintenance of the existing systems, as well as set the security standards which must be complied with.

5.4 SECURITY REQUIREMENTS

When developing or changing systems, the product owner and the engineer document the Security Requirements Specification on tickets, including a security risk assessment and steps to implement to mitigate the risk.

5.5 CHECKING AND TESTING THE IMPLEMENTATION OF SECURITY REQUIREMENTS

The C.T.O. is responsible to define the methodology, responsibilities and the timing of checking whether all the security requirements from the Security Requirements Specification have been met, and whether the system is acceptable for production.

The security testing consists of internal security testing during development with automated tests, code analysis tools, code reviews, and QA performing acceptance tests against the Security Requirements Specification, and external, independent penetration tests.

5.6 Repository

TinQwise uses GitLab as the repository for code and version control. The use of the repository (access rights, etc.) is regulated in the Access Control Policy. The Head of Engineering will issue procedures for using git.

5.7 Version control

The use of git for version control, including branching strategies and tagging of releases is described in the procedures for using git.

Release numbering uses the Semantic Versioning "CALVER" format: year.week.revision (2023.45.2.2.16 for example)

- "year" is the year of the release.
- "week" is the week of the last major release release.
- "Revision" increments every time a new version is deployed to production.

5.8 Change control

Changes in the development and during the maintenance of the systems must be done according to Change Management Policy.

5.9 Protection of test data

Confidential data, as well as data that can be related to individual persons must not be used as test data. The types and use of test data is described in the procedures for Secure Engineering Principles.

5.10 Required Security Training

The C.O.O & C.T.O define the level of security skills and knowledge required for the development process and ensure training is in place.

5.11 Information about secure development procedures and practices for customers

For any information required by Client regarding the development process, the C.O.O. must decide whether such information can be sent according the Information Classification Policy.

6. 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

7. 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.	TinQwise Staff can access these files	2 years for lists that are no longer valid
Procedures for secure information system engineering and secure development lifecycle	SharePoint and / or GitLab	C.T.O.	TinQwise Staff can access these files	2 years for procedures that are no longer valid
Pentest and other security test reports	SharePoint	C.O.O & C.T.O	Only TinQwise Staff can access these files	5 years