Version 2026.07

TinQwise Policy

003.4
Change Management

TinQwise B.V. | Mussenstraat 15 | 1223 RB | Hilversum | The Netherlands | +31 35 538 5656
CoC Hilversum 32082603 | VAT NL809771287B01 | IBAN NL26 INGB 0006679651 | SWIFT / BIC INGBNL2A | tinqwise.com

tinQwise

Validity and document management

Version	Date	Author	Description
01	01/01/2021	Simon Kennedy	Document creation
02	28 /10/ 2021	Simon Kennedy and Emil de Valk	Annual review and policy update.
03	31/10/2022	Simon Kennedy, Emil de Valk and Elena Neagu	Annual review and policy update.
04	28/11/2022	Emil de Valk and Reinoud van Dommelen	Update to align with standard customer contract set. Definitions, renumbering and consistency.
05	02/11/2023	Emil de Valk and Okke Formsma	Annual review & update
06	11/12/2024	Emil de Valk	Annual review
07	28/11/2025	Emil de Valk	Annual review

This document is valid as of January 1st, 2026.

The owner of this document is the C.E.O., 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) support requests arising from failed security controls built into the systems

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

You may not copy or transmit the contents of this document either electronically or in hard copies, nor may the document be altered in any manner. The latest version of this policy is available at https://www.tinqwise.com/policies/change-management. If you are interested in using the contents of this document in any form, please contact TinQwise via info@tinqwise.com with details of your request.

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	X

2. Purpose

The purpose of this policy is to ensure that all changes to TinQwise Platform minimize any potential negative impact on services and Users.

3. Scope

The change management policy, and all policies referenced herein, apply to all employees, contractors, consultants, temporary, and other workers at TinQwise (the "User(s)") who use, access, or otherwise employ, locally or remotely, TinQwise resources, whether individually controlled, shared, stand-alone, or networked.

4. Reference documents

Related policies, processed and procedures:

- 002.1 TinQwise ISRMS Governance Policy
- 003.2 TinQwise Data Privacy Policy
- 003.3 TinQise Secure Development Policy
- 004.1 TinQwise Access Control Policy

5. Policy Statement

- Submitting & validating change requests
    - Change requests must always be submitted via the product owner
    - Change requests undergo a rigid validation and impact assessment prior to implementation
    - Implementing changes must always follow OWASP standard guidelines
    - Changes must be vetted for security implications through the participation of the Security Officer as part of the Security Requirements Specification.

- Change management in code (see Figure 1: Change management from code repository perspective)
    - All code repositories follow the Gitflow pattern to have stable, releasable versions and rollback possibilities in place
    - When releases are prepared, this always follows the gitflow release flow, both for hotfixes and regular scheduled releases
    - All code repositories adhere to the Calendar versioning pattern (year.week.revision)
- Urgent changes
    - Urgent changes will be picked up per the service management policy and general SLA guidelines
    - In case of urgent changes, a Hotfix change will be prepared by an appointed developer.
    - A hotfix will always be reviewed by a reviewer.
    - After approval the hotfix will be validated on an appropriate test environment before deployment to production
    - Hotfixes always use a Revision version (e.g. 2025.01.1)
- Regular minor changes
    - Changes are released via bi-weekly minor releases
    - Changes are tracked in changelogs
    - Changes are communicated with internal stakeholders prior to release
    - Changes are widely communicated with external stakeholders after release
- Product development and major changes
    - Changes are communicated at least 1 calendar month ahead of release
    - Changes are released via bi-weekly release process
    - Large changes are introduced with feature enablement, allowing gradual rollouts
    - In most major changes' customers should be able to opt out
- Code reviews
    - TinQwise enforces a Four Eyes Principle, requiring all changes, including code, configurations, and deployments, to undergo peer review to ensure security, quality, and compliance.
    - Merge requests are documented and assigned to qualified reviewers in Gitlab.
    - Review activities are logged for transparency, and exceptions allowed only under emergency protocols with senior approval and retrospective review.
- Maintenance windows
    - If a change required taking critical portions of the infrastructure offline for a maintenance window, this will be communicated to impacted customers at least 48 hours prior to the start of the window.
    - Maintenance windows will be scheduled outside office hours Central Europe time
    - Maintenance windows are always communicated via status.tinqwise.com.
- Quality assurance
    - Prior to bi-weekly releases extensive QA testing is performed
    - Automated test facilities are in place to ensure backwards compatibility and to avoid regression problems

- Bi-weekly releases (see Figure 2: Change management from release timeline perspective)
    - Bi-weekly releases are deployed as a rolling update over the entire infrastructure, without downtime unless that is impossible
    - Rollback procedures are in place in case of a faulty release.
    - Bi-weekly releases use a year and week number version number (e.g. 2025.1.0).
- Change management communications
    - Product changes are demonstrated every month in an Ask me Anything webinar for Clients
    - Product changes are communicated every month in a product update newsletter for Clients
    - Product changes are documented in assistive articles accessible for all Clients via docs.tinqwise.com and their TinQwise Platform
- Account level change management
    - Every customer can request access to a sandbox environment (QA) to validate pre-release versions.
    - Customer success representatives will assist customers with implementing major changes in their account

6. Process visuals

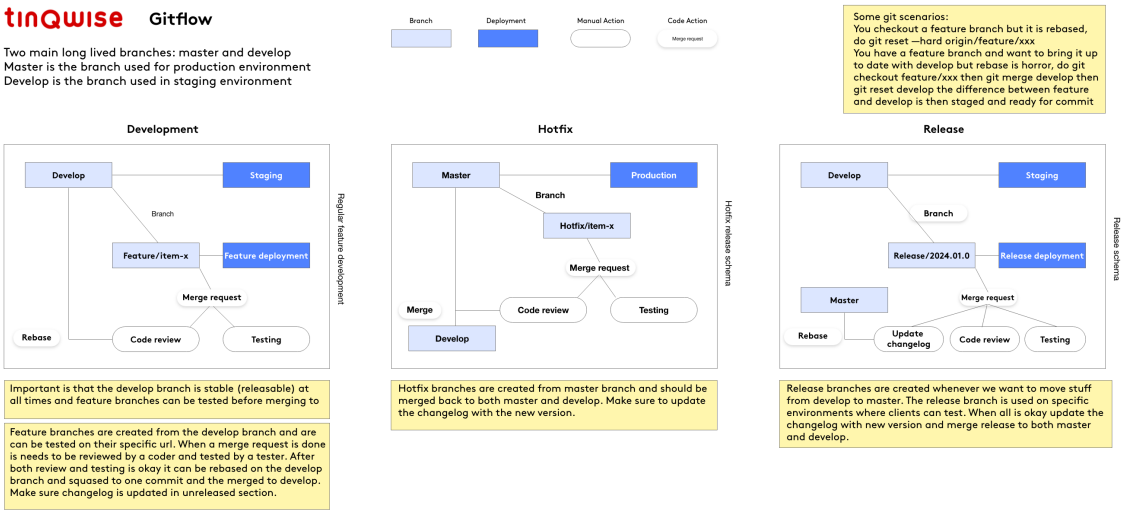

Figure 1: Change management from code repository perspective

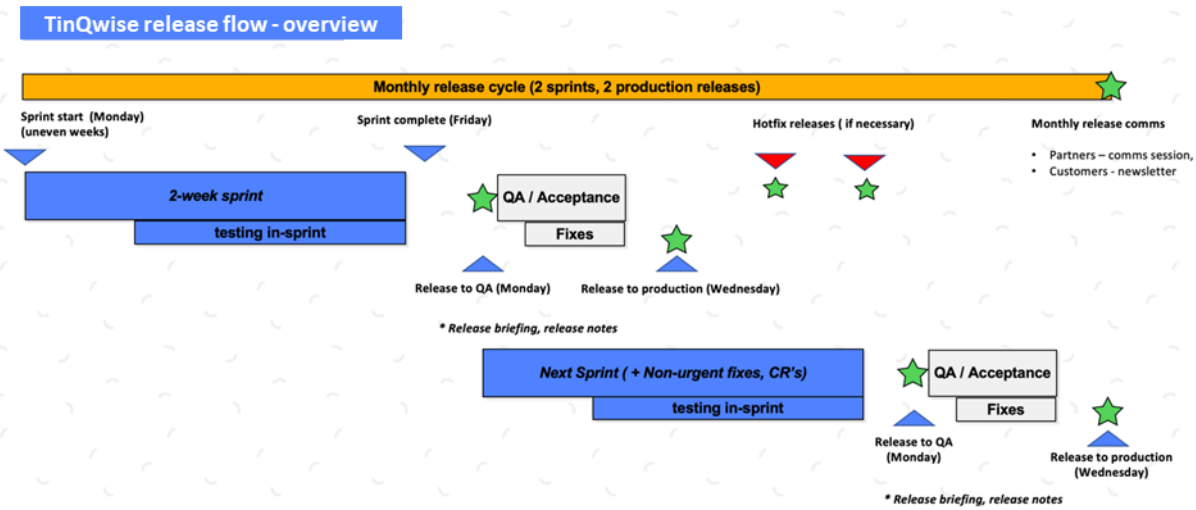

Figure 2: Change management from release timeline perspective

7. Compliance to this policy

The C.E.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 ISRMS process as defined in the ISRMS Governance policy.

8. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Change requests	SharePoint, Productboard and / or GitLab	C.E.O.	Only team members can access these files	2 years
Pentest and other security test reports	SharePoint	C.E.O.	TinQwise Staff can access these files	2 years for tests that have been performed