Version 2025.07

TinQwise Policy

004.2

Asset 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
1	2021-03-31	Simon Kennedy	Document creation
2	2021-10-26	Simon Kennedy	Annual review and policy update
3	2022-11-03	Simon Kennedy, Stein Grubben and Elena Neagu	Annual review and policy update
5	2023-03-09	Emil de Valk and Reinoud van Dommelen	Update to align with standard customer contract set. Definitions, renumbering and consistency.
6	2023-11-09	Simon Kennedy and Okke Formsma	Annual review and policy update
07	2024-12-11	Emil de Valk	Annual review, add BYOD statement

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

The owners of this document are the C.O.O., who must check and, if necessary, update the document at least once a year, or earlier if material changes in organisation structure such as M&A occur.

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

- Consistency of application of asset management
    - End user hardware;
    - Cloud servers and infrastructure;
    - Software.
- Completeness of coverage of asset management and asset registers.
- Consideration of technological innovations and completeness – e.g. serverless infrastructure.

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/asset-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	X

2. Purpose

This policy document defines the approach to Asset Management for software and hardware assets implemented by TinQwise.

It informs staff about processes and procedures regarding Information Technology Asset Management. This policy establishes and enforces technical and administrative controls to support asset management, both in internal operations and as applicable to cloud infrastructure assets hosting TinQwise Platform instances of our customers. This is an evolving policy and will be updated as needed.

3. Scope

Information Technology Asset management at TinQwise is divided into 3 categories:

1. Hardware assets (limited to employee laptops, mobile phones, printers and associated hardware)
2. Cloud infrastructure (e.g. (virtual) servers for hosting the TinQwise platform)
3. SaaS (3rd party software assets managed by SaaS providers.)

This policy covers specifically items 1, 2 & 3. Items 1 and 3 are managed by the IT Service Provider. Item 2 is managed directly by TinQwise product organisation and DevOps engineers under leadership of the H.o.E. and the C.O.O.

The C.O.O. is responsible for ensuring that all assets are distributed, controlled, managed and disposed of in a controlled and concise manner following correct security and asset management procedures.

tinQwise

4. hardware assets

Hardware assets are managed by the IT Service Provider as the responsible party, and all hardware assets are registered and tracked via the System of Record that is operated by the IT Service Provider of TinQwise, in accordance with our Access Control Policy.

5. Cloud infrastructure assets

TinQwise makes use of a Cloud Service Provider for all hosting, deployment, pipeline, and all services required to successfully run TinQwise Platform as a fully scalable SaaS application. The C.O.O. and Head of Engineering are the responsible parties.

All assets with regards to the Cloud Service Provider are managed and registered via the System of Record of that Cloud Service Provider.

https://eu-west-1.console.aws.amazon.com/console/home?region=eu-west-1#

6. (SAAS) software assets

The majority of applications used by TinQwise are SaaS applications. These are managed by the IT Service Provider, and all software assets are registered and tracked via the System of Record that is operated by the IT Service Provider of TinQwise, in accordance with our Access Control Policy.

7. Asset Usage & Security: Bring Your Own Device (BYOD)

Employees are permitted to use personal devices to access TinQwise systems, provided these devices meet the security requirements defined in this policy. To ensure compliance and protect organizational assets, all BYOD devices must be registered with the IT department prior to use and configured to align with TinQwise's security standards.

TinQwise reserves the right to audit and enforce security measures on all registered BYOD devices. These measures include, but are not limited to, verifying compliance with security configurations and performing remote wiping of corporate data if necessary to protect company information or in the event of a security incident.

8. Asset management roles and responsibilities

C.O.O.

The C.O.O. ensures safe, secure and consistent asset management through:

- Ensuring correct roles and responsibilities are documented and monitored regarding maintenance of asset registers and consistent use of software assets.
- Regular review to endure asset registers in the systems of record are accurate and up to date.

- Monitoring and improving the process and ensuring changes in the organization and technology landscape are accurately reflected and documented in the systems of record.
- Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibilities.

Employees of the IT Service Provider

The Employees of the IT Service Provider are responsible for:

- Day-to-day asset operations, particularly regarding end-user hardware and software applications.
- Maintaining the hardware and software asset registers.
- Monitoring and logging ownership and usage of hardware and applications.
- Ensuring appropriate usage according to policy.
- Ensuring operational status and coverage of anti-malware software and other security measures.
- Safe and secure network operations (excluding Cloud Infrastructure).
- Following up with system administrators for the identification, testing, distribution, deployment and implementation of technical configurations, and requirements if appropriate.
- Investigating any network security or hardware-related incident, event or behaviour.

C.O.O. and Head of Engineering

The C.O.O. and Head of Engineering are responsible for:

- Day-to-day cloud infrastructure operations, particularly w.r.t secure operations and uptime.
- Maintaining the cloud infrastructure asset register.
- Monitoring and logging ownership and usage of cloud infrastructure.
- Ensuring appropriate usage according to policy.
- Ensuring operational status and coverage of security measures.
- Safe and secure cloud infrastructure network operations.
- Investigating any network security or hardware-related incident, event or behaviour.
- Categorizing, reporting, analysing, responding and escalating performance- or application stability-related incidents.

9. 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 or employee of the IT Service Provider, found to have violated this policy, may be subject to disciplinary action, up to and including termination of employment or contract.

tinQwise

10. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Incident reports	SharePoint and / or GitLab	C.O.O.	TinQwise Staff	5 years
Pentest and other security test reports	SharePoint	C.O.O.	TinQwise Staff	5 years
Cloud asset register	Console of Cloud Service Provider: https://eu-west-1.console.aws.amazon.com/console/home?region=eu-west-1#	C.O.O	TinQwise Staff	5 years
Hardware register	Infrastructure management portal of IT Service Provider	Account manager of IT Service Provider	Only employees of IT Service Provider can access these files	5 years
(Saas)Software usage register	Infrastructure management portal of IT Service Provider	Account manager of IT Service Provider	Only employees of IT Service Provider can access these files	5 years