Version 2025.07

TinQwise Policy

004.1

Access Control

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	18/02/2020	Simon Kennedy	Document creation
02	24/11/2020	Simon Kennedy	Annual review and policy update. Major updates based on organisation changes and updated procedures
03	27/10/2021	Simon Kennedy and Emil de Valk	Annual review and policy update. Key updates based on tightened access control procedures
04	03/11/2022	Simon Kennedy, Emil de Valk, Okke Formsma and Elena Neagu	Annual review and policy update.
05	09/03/2023	Emil de Valk and Reinoud van Dommelen	Update to align with standard customer contract set. Definitions, renumbering and consistency.
06	02/11/2023	Simon Kennedy and Reinoud van Dommelen	Yearly review and update. Adjusted wording, aligned more closely with ISO 27001:2023 norm. Added Physical Access. Changed info@tinqwise.nl into info@tinqwise.com.
07	11/12/2024	Emil de Valk	Annual review, explicitly add “Access management” and “least privileged principle” clauses

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

The owner of this document is the C.O.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) incidents arising from failed security controls built into the systems
- 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	X	X	X

2. Purpose

This policy outlines the requirements for control of access to TinQwise's information systems. The purpose of access control in the context of TinQwise's information security risk management system (ISRMS) is to:

- Limit and regulate access to information systems and information processing facilities;
- Ensure authorised user access and to prevent unauthorised access to information systems and information processing facilities;
- Make users accountable for safeguarding their authentication information; and
- Prevent unauthorized access to information systems and information processing facilities.
- Ensure compliance with GDPR / AVG standards and customer contractual requirements for data protection.

3. Scope

This policy applies to all information systems in scope of TinQwise's Information Security & Risk Management System. A more detailed description of the scope is included in the ISRMS scope document (please refer to 002.1 ISRMS Governance).

All TinQwise Staff (for definition please refer to 00 Roles & Definitions) are responsible for exercising good judgment regarding appropriate use of information systems that are in scope in accordance with TinQwise's Policies, standards, and local laws and regulation.

4. Reference documents:

4.1 Related policies, processes and procedures

- 000 Roles & Definitions
- 002.1 TinQwise ISRMS Governance Policy
- 003.3 TinQwise Secure Development Policy

4.2 Relevant ISO27001:2013 clause(s):

- Annex A 9.1.1 Access control policy. An access control policy should be established, documented and reviewed based on business and security requirements.
- Annex A 9.1.2 Policy on the use of network services. Users should only be provided with access to the network and network services that they have been specifically authorized to use.
- Annex A 9.2.1 User registration and de-registration. A formal user registration and de-registration process should be implemented to enable assignment of access rights.
- Annex A 9.2.2 Privilege management. A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.
- Annex A 9.2.3 Management of privileged access rights. The allocation and use of privileged access rights should be restricted and controlled.
- Annex A 9.2.4 Management of secret authentication information of users. The allocation of secret authentication information should be controlled through a formal management process.
- Annex A 9.2.5 Review of user access rights. Asset owners should review users' access rights at regular intervals.
- Annex A 9.2.6 Removal or adjustment of access rights. The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.
- Annex A 9.3.1 Use of secret authentication information. Users should be required to follow the organization's security practices in the use of secret authentication information.
- Annex A 9.4.1 Information access restriction. Access to information and application system functions should be restricted in accordance with the access control policy.
- Annex A 9.4.2 Secure log-on procedures. Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.
- Annex A 9.4.3 Password management system. Passwords management systems should be interactive and should ensure the quality of passwords.
- Annex A 9.4.4 Use of privileged utility programs. The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.
- Annex A 9.4.5 Access control to program source code. Access to program source code should be restricted.

5. MINIMUM REQUIREMENTS

5.1 User Access Management

- Access to TinQwise's information systems is based on the least privileges required to perform job responsibilities.

- The formal user registration and de-registration procedure is implemented to enable assignment and revocation of access rights to TinQwise's information systems. This is part of TinQwise's standard onboarding and offboarding processes.
- The formal user registration and de-registration procedure include that any access of internal users (i.e., TinQwise Staff, so including external users, such as external suppliers to TinQwise's information systems requires explicit approval by the respective Team Lead before a user access is granted.
- User IDs are not reassigned to another user.
- Users are identified through a unique user account that is unambiguously tied to the individual. Generic users such as service@tinqwise.com / office@tinqwise.com / facturen@tinqwise.nl can only by accessed by individuals and are made solely for continuity purposes.
- The use of generic or group access accounts to access TinQwise's information systems is strictly prohibited.
- The provisioning of secret authentication shall be controlled through a formal procedure.
- Departmental managers are responsible to ensure that user access rights for in scope information assets are reviewed at regular intervals and acted upon when required.
- The access rights of all internal users (i.e., employees, contractors, consultants, temporary, and other workers at TinQwise) to TinQwise's information systems shall be revoked and removed upon termination of their employment, contract or agreement or adjusted upon change.
- Any accounts used by external users to access, support and maintain TinQwise's information systems shall be disabled by default, and enabled only when needed.
- HR and TinQwise IT service provider shall ensure that access rights of external users are revoked and removed upon termination of their contract agreement or adjusted upon change.
- Revealing secret authentication information and the sharing of secret authentication information across multiple users is not allowed.

5.2 User authentication

- A suitable authentication method that is appropriate to the level of information classification shall be implemented for TinQwise's information systems.
- For (each) authentication method, a secure log-on procedure shall be defined and implemented to minimise unauthorised access to TinQwise's information systems.
- Secure logon procedures shall (amongst others):
    - Disclose the minimum information about the information system;
    - Number of attempts before the device is locked out; and
    - Maximum time interval for a user to re-authenticate and re-activate an idle session.
- Any authentication method implemented by TinQwise shall ensure that user authentication information shall be stored and transmitted in a protected form.

5.3 Password Management

- When a password is used as an authentication method, a procedure is defined and implemented that:
    - Allow users to select and change their own passwords;
    - Include a confirmation procedure to allow for input errors;
    - Enforce a choice of quality passwords;
    - Force users to change their initial (first-time) passwords for the first time they use the password;
    - Enforce both initial (first-time) passwords for new users, and reset passwords for existing users to be set to a unique value for each user;
    - Enforce regular passwords changes;
    - Enforce validation of the identity of the user requesting password reset before performing password resets;
    - Prevent re-use of previously used passwords when changing the password; and
    - Not display passwords on the screen when being entered.
- All user-level and system-level credentials conform to the requirements documented in the procedure.
- Users do not use the same password for TinQwise accounts as for other non- TinQwise access (for example, personal accounts, third-party portals, etc.).
- Where possible, users do not use the same password for various TinQwise access needs, and preferably shall use Single Sign on.
- Where single-sign on is not available, users use TinQwise's standard and centrally managed password management application '1password' only.
- User accounts that have system-level privileges granted through group memberships or programs, such as root, have a unique password from all other accounts held by that user to access system- level privileges.
- All system-level passwords (for example root, AD admin, application administration accounts, and so on) are changed regularly.
- Passwords are not stored in plaintext or in any easily reversible form.
- Passwords are not to be transmitted over unencrypted channels.
- Passwords are not to be shared with anyone, both within TinQwise and outside TinQwise, unless authorised.
- Users do not change their password to one suggested by another party.
- Users do not hint at the format of a password (for example, "my family name").
- Users do not keep a record (e.g., post-it, paper, software file) of passwords, unless this can be stored securely, and if so, will only use TinQwise's standard and centrally managed password management application '1password'.
- Users change their password as soon as any indication of possible system or password compromise is discovered or suspected and inform the Security Committee.
- Users do not include passwords in an automated log-on process (such as a script).

5.4 Privileged Access

- A procedure is defined and implemented for the allocation and use of privileged access rights (e.g., administrator access) that addresses:
    - Limitation of the use of privileged access rights to the minimum practical number of trusted, authorised users;
    - Authorisation for ad hoc users of privileged access rights;
    - Logging of and reviewing the activities of users with privileged access rights; and
    - Segregation of duties between end-user access and privileged user access.
- The allocation and use of privileged access right (e.g., administrator access) are controlled and monitored.

5.5 Remote access

- Whenever remote access is authorised, it is controlled through use of multi-factor authentication mechanisms.
- All communications transfer through uncontrolled infrastructure, that are used for accessing TinQwise's information systems is only accessible through a secure tunnelling connection.
- While remotely connected to TinQwise's network, users must ensure their device is not connected to any other network at the same time, except for personal networks that are under their complete control or under the complete control of a trusted third party.

5.6 Access review

TinQwise conducts monthly access reviews to ensure that all access permissions, particularly privileged accounts, are aligned with users' roles and responsibilities. These reviews verify the necessity of access levels, ensuring they are appropriate for the tasks required. Inactive accounts or those no longer required are promptly identified and deactivated to minimize risks.

Additionally, access is revoked immediately for users who change roles, leave the organization, or no longer require privileged access.

5.7 Least Privilege Principle

TinQwise implements the Least Privilege Principle to ensure that users, applications, and systems are granted the minimum level of access required to perform their duties effectively. Access permissions are carefully assigned to limit exposure to sensitive data and critical systems, reducing the potential for misuse or accidental compromise.

Access rights are reviewed regularly and adjusted as roles or responsibilities change to maintain alignment with operational needs. Privileged access is restricted to those with a demonstrated need, and any elevated access is granted on a temporary basis with appropriate oversight.

tinQwise

6. Physical Access

TinQwise maintains a no-paper policy. All data is stored electronically in our cloud systems, and only if necessary, on secured end point devices. All machines are encrypted and password protected. Network hardware is secured in a locked room. We handle a clean desk and locked screen policy. In this way, physical access risk, related to unauthorised persons at TinQwise office locations, is mitigated.

TinQwise Platform and data is hosted by Amazon Web Services (AWS), the world's largest and most reliable cloud service provider, in ISO27001, ISO27002, and SOC 2-compliant data centres. Physical access is controlled upon entry to access points by professional security personnel using surveillance, detection systems and other electronic means. Authorized personnel uses multi-factor authentication mechanisms to access data centres. Server room entrances are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

Electronic intrusion detection systems are installed in the data layer to monitor, detect, and automatically alert the appropriate personnel of security incidents. Entry and exit points to server rooms are secured with devices that require everyone to provide multifactor authentication before granting entry or exit. These devices will give alarms if the door is forced or left open without authentication. Door alarm devices are also configured to detect instances where an individual leaves or enters a data layer without providing multi-factor authentication. Alarms are immediately sent to 24/7 AWS Security Operations Centres for instant logging, analysis and response.

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
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 for procedures that are no longer valid