Version 2025.06

TinQwise Policy

003.1

Security Incident 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	2020-11-10	Simon Kennedy	Document creation
02	2021-10-28	Simon Kennedy & Emil de Valk	Annual review and policy update.
03	2022-11-03	Simon Kennedy, Emil de Valk, Okke Formsma	Annual review and policy update.
04	2023-03-09	Emil de Valk and Reinoud van Dommelen	Review in line with the Data Protection Terms a spart of our Agreements with our Clients. Definitions, renumbering and consistency.
05	2023-11-02	Emil de Valk and Okke Formsma	Annual review and policy update
06	2023-12-11	Emil de Valk	Annual review & update

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

The owner of this document is the C.O.O., 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 bi-annual security 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

2. Purpose

The purpose of this document is to outline the information security requirements regarding Information Security Incident Management within TinQwise. These rules are in place to ensure that information security requirements to mitigate risks related to information security incidents are agreed upon; documented, implemented and effectively enforced.

In addition, this document must guarantee a perfect operation in line with the data protection agreements with TinQwise's Clients. The standard terms can be found in TinQwise Data Processing Terms.

3. Scope

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

TinQwise Staff are responsible for exercising good judgment regarding appropriate use of information systems that are in scope in accordance with TinQwise policies, standards, and local laws and regulation.

4. Reference documents:

4.1 Rrelated policies, processes and procedures

- 003.1 Security Incident Management Policy
- 003.2 TinQwise Data Privacy Policy
- 003.3 TinQwise Secure Development Policy
- 004.1 TinQwise Access Control Policy

4.2 Relevant ISO27001:2013 clause(s):

- Annex A 16.1.1 Responsibilities and procedures. Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
- Annex A 16.1.2 Reporting information security events. Information security events shall be reported through appropriate management channels as quickly as possible.
- Annex A 16.1.3 Reporting information security weaknesses. Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
- Annex A 16.1.4 Assessment of and decision on information security events. Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents.
- Annex A 16.1.5 Response to information security incidents. Information security incidents shall be responded to in accordance with the documented procedures.
- Annex A 16.1.6 Learning from information security incidents. Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
- Annex A 16.1.7 Collection of evidence. The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

5. Minimum requirements

5.1 Roles and responsibilities

- C.O.O. and Head of engineering are responsible for ensuring all technical monitoring and tooling is in place to prevent potential security incidents, and track, log and monitor suspicious behaviour in our applications.
- Team Leads are responsible for ensuring that all TinQwise Staff are aware of the requirements for reporting information security events and incidents as outlined in this standard.
- All TinQwise Staff are responsible for reporting information security events and incidents per the requirements as outlined in this standard as quickly as possible.
- An information security reporting procedure is defined and implemented and communicated to all TinQwise Staff
- The Security Committee is responsible for the actual management of security incidents.
- Access to information relating to specific information security incidents must only be given on a need- to-know basis.

5.2 Assessing information security incident

The following steps will be taken:

- A reporting channel must be made available to TinQwise's employees, contractors, consultants, temporary, and other workers to report information security events and incidents.
- At a minimum, the following information must be provided as part of an information security incident report:
    - Description of the incident;
    - When the incident was discovered;
    - When the incident occurred (when available);
    - Where the incident occurred (where applicable);
    - Details of the person reporting the incident;
    - Whether the incident concerns a near miss or actual incident;
    - What information is involved;
    - The classification level of the information;
    - Preliminary assessment of impact on information security; and
    - Immediate cause of the incident (when available).
- Information security events and incidents must be reported exclusively to the C.O.O. and to the Security Committee in their absence.
- The Security Committee is responsible for assessing whether the reported event should be identified as an information security incident.
- The Security Committee is responsible for assessing the information security incident and classifying it in terms of:
    - Impact – damage caused by the incident to TinQwise (reputation, financial, disruption of business processes, etc.);
    - Potential impact on Clients or Clients' data
    - Urgency – the speed with which the incident is to be corrected.
- The Security Committee must report the assessment of the information security incident to the C.O.O.

5.3 Responding to information security incidents

The following responsibilities are taken:

- The C.O.O. is responsible for escalating the incident and initiating emergency response as required.
- The Security Committee is responsible for collecting and logging relevant evidence for the information security incident as soon as possible.
- A procedure is defined and implemented that outlines the requirements for identification, collection, acquisition and preservation of evidence, considering:
    - Chain of custody;
    - Confidentiality, integrity and availability of evidence;
    - Safety of employees, contractors, consultants, temporary, and other workers;
    - Documentation;
    - Legal requirements.

- The C.O.O. is responsible for communicating the existence of the information security incident or any relevant details thereof to internal stakeholders with a need to know after a review by the Security Committee.
- The C.O.O. is responsible for communicating the existence of the information security incident or any relevant details thereof to external stakeholders with a need to know after an approval by the Security Committee and the M.T..
- The H.o.E. together with the D.P.O. are responsible, supported by the Security Committee, for identifying required activities for correcting the information security incidents and monitoring timely follow-up of those.

5.4 Learning from information security incidents

A root cause analysis must be performed for information security incidents and lessons learned must be identified to reduce the likelihood and impact of similar incidents in the future.

The Security Committee, together with the Team Leads (where appropriate), are responsible for implementing the mitigating measures resulting from lessons learned.

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.

7. 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	Head of Engineering.	Secure SharePoint. Only Security Committee can access these files.	5 years
Pentest and other security test reports	SharePoint	C.O.O.	Secure SharePoint. TinQwise Staff can access these files	5 years