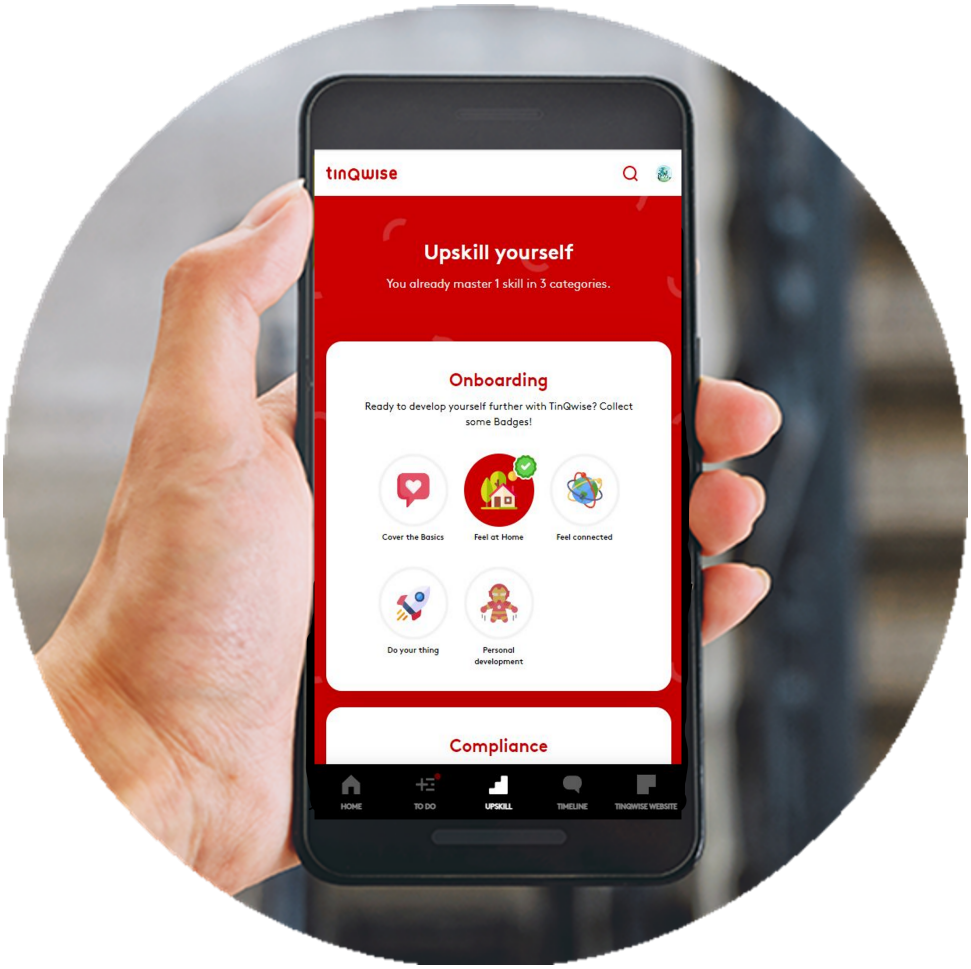
Version 2024.01

# TinQwise Policy




# 005.2 Information Classification

tinQwise

## VALIDITY AND DOCUMENT MANAGEMENT

| Version | Date | Author | Description |
|---|---|---|---|
| 01 | 01/04/2023 | Simon Kennedy & Liselotte Pröpper | Document creation |
| 02 | 02/11/2023 | Simon Kennedy & Liselotte Pröpper | Annual review and policy update. |

This document is valid as of December 1, 2023.

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 (potential) data classifications related findings arising from regular and ad-hoc security reviews and penetration testing.
- Number of (potential) data classification / data security incidents arising from failed security / access 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



## 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

The purpose of this document is to offer a detailed overview of how we classify information for the purpose of safeguarding company and customer data safely, structurally, and by design. This policy is designed to align with ISO 27001:2023 standards to ensure the confidentiality, integrity, and availability of our data assets.

This Information Classification Policy will be reviewed annually or as needed to ensure it remains aligned with ISO 27001:2023 standards and the evolving needs of TinQwise.

## 3. SCOPE

This policy applies to all employees, contractors, and third parties who have access to TinQwise's and our customers data. It covers all data stored, processed, and transmitted by the organization, with a primary focus on data within the TinQwise growth platform.

## 4. REFERENCE DOCUMENTS:

### 4.1 RELATED POLICIES, PROCESSES AND PROCEDURES

- 002.1 TinQwise ISRMS Governance
- 003.1 TinQwise Security Incident Management Policy
- 003.2 TinQwise Data Privacy Policy
- 003.3 TinQwise Secure Development Policy
- 004.1 TinQwise Access Control Policy
- 005.1 TinQwise Data Segregation & Retention

tinQwise

## 5. COMPLIANCE TO THIS POLICY

TinQwise's Information Classification Policy is a fundamental component of our information security framework. Adherence to this policy is mandatory, and all employees and stakeholders must understand their roles and responsibilities in preserving the confidentiality, integrity, and availability of our data assets.

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.

## 6. CLASSIFICATION CATEGORIES AND DATA OWNERS

TinQwise classifies data into the following categories based on their sensitivity and the potential impact of unauthorized disclosure, modification, or destruction. Each category of data will have designated data owners, responsible for overseeing access, protection, and classification. Data owners will be identified for every data type and mentioned behind each type.

### 6.1 Public Data (Category 1):

This category encompasses information that is intended for public consumption without any restrictions. Public data is not considered sensitive and can be openly shared with no or minimal controls. It includes:

- Marketing materials: Brochures, advertisements, press releases, and promotional content that are meant for public dissemination. Head of Marketing (H.o.M) is data owner.
- Public-facing website content: Information that is accessible to anyone visiting a website, such as general company information, blogs, and news updates. H.o.M. is data owner.
- Social Media content: Social media platforms often contain public data, such as public posts, tweets, and public profiles that are accessible to anyone. H.o.M. is data owner.
- Non-sensitive operational documents: Documents that are widely shared within the organization but contain no sensitive or confidential information, like general company policies and guidelines. C.O.O. is data owner.
- General internal communication: Information intended for all employees, such as company-wide announcements or non-sensitive internal newsletters. Head of Human Resources (H.o.HR) is data owner.

### 6.2 Internal Data (Category 2):

Data within this category is for internal use only and should not be shared externally. While not as sensitive as confidential or restricted data, it still requires careful handling. Internal data includes:

- Employee handbooks: Documents outlining company policies, procedures, and guidelines for internal use. H.o.HR is data owner.

- Non-sensitive operational documents: Documents that are primarily used internally but may not be suitable for public consumption. Team Leads are data owners.
- General internal communication: Information intended for all employees, as described above, but not intended for external parties. H.o.HR is data owner.

### 6.3 Confidential Data (Category 3):

This category includes highly sensitive information that requires strict access control and protection measures. Unauthorized access or disclosure could lead to significant harm to TinQwise and our customers. Confidential data includes:

- Customer data: Personal information, financial data, and any customer-specific information that is not intended for public knowledge. Data Protection Officer (D.P.O.) is data owner.
- Financial information: Sensitive financial reports, budget details, and financial forecasts. C.F.O. is data owner.
- Intellectual property: Proprietary information, trade secrets, patents, copyrights, and confidential business strategies. C.T.O. is data owner.
- Data subject to legal or regulatory requirements: Information that must be protected according to legal or industry-specific regulations, such as HIPAA for healthcare or FERPA for education. C.F.O. is data owner.

### 6.4 Restricted Data (Category 4):

The most sensitive data belongs to this category and demands the highest level of protection and control. Access to restricted data is strictly controlled and monitored to prevent any unauthorized access or disclosure. Restricted data includes:

- Personally identifiable information (PII): Data that directly or indirectly identifies individuals, such as social security numbers, credit card information, and medical records. D.P.O. is data owner.
- Proprietary source code: The core codebase of our software products and other intellectual property. C.T.O. is data owner.
- High-risk Assets: Any information or data that, if compromised, could result in severe financial, legal, or reputational damage to TinQwise or our customers. Security committee is data owner.

These classification categories are essential for guiding employees and stakeholders on the appropriate handling, storage, and protection of data based on its sensitivity and importance. The data owner for each system or database containing data from these categories is responsible for ensuring that the appropriate security measures and access controls are in place.

tinQwise

# 7. DATA HANDLING AND CLASSIFICATION PROCEDURES

## 7.1 DATA CLASSIFICATION PROCESS

The classification of data should be initiated when it is created or received. The process includes:

1. Determining the data category as outlined in Section 6.
2. Designating a data owner responsible for maintaining and protecting the data.
3. Ensuring that data is properly labelled and tagged to reflect its classification.
4. Continuously reviewing and updating the classification based on changes in the data's sensitivity.

## 7.2 HANDLING AND ACCESS CONTROL

Access to data is restricted based on its classification. Access rights will be assigned and revoked as necessary. Employees must adhere to the principle of "need-to-know" when accessing and using data. Encryption, authentication, and authorization mechanisms are employed to safeguard data in transit and at rest. More details our stated in our TinQwise Access Control Policy and Secure Development Policy.

## 7.3 DATA STORAGE AND RETENTION

Data storage and retention are determined based on its classification and relevant legal and regulatory requirements. Data should be stored securely in accordance with our data protection standards stated in our Data Segregation & Retention policy.

## 7.4 DATA TRANSMISSION

Data in transit is protected through encryption and secure communication protocols.
Only authorized individuals may transmit confidential or restricted data.

# 8. TRAINING AND AWARENESS

All employees are required to undergo data classification training. Data owners are responsible for raising awareness about the importance of data classification within their teams.

# 9. AUDITING AND COMPLIANCE

Regular audits and assessments will be conducted to ensure compliance with this policy.
Non-compliance may result in disciplinary action and/or legal consequences.

# 10. INCIDENT RESPONSE

A well-defined incident response plan is in place to address data breaches and incidents. All data breaches are reported promptly to the relevant authorities and affected parties as required by law. See more details of the plan in our TinQwise Security Incident Management Policy.

tinQwise

## 11. 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 information classification | SharePoint | C.O.O. | Only team members can access these files | 2 years for procedures that are no longer valid |