Data Management Policy

Policy Owner: Pedro Piñera Buendía

Effective Date: Oct 23, 2024

Purpose

To ensure that information is classified, protected, retained and securely disposed of in accordance with its importance to the organization.

Scope

All Tuist GmbH data, information and information systems.

General requirements

Tuist GmbH classifies data and information systems in accordance with legal requirements, sensitivity, and business criticality in order to ensure that information is given the appropriate level of protection. Data owners are responsible for identifying any additional requirements for specific data or exceptions to standard handling requirements.

Information systems and applications shall be classified according to the highest classification of data that they store or process.

Data classification

To help Tuist GmbH and its employees easily understand requirements associated with different kinds of information, the company has created three classes of data.

Confidential
Highly sensitive data requiring the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner, or a company executive. Examples include:

- Customer Data
- Personally identifiable information (PII)
- Company financial and banking data
- Salary, compensation and payroll information
- Strategic plans
- Incident reports
- Risk assessment reports
- Technical vulnerability reports
- Authentication credentials
- Secrets and private keys
- Source code
- Litigation data

Restricted
Tuist GmbH proprietary information requiring thorough protection; access is restricted to personnel with a "need-to-know" based on business requirements. This data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise. Examples include:

- Internal policies
- Legal documents
- Meeting minutes and internal presentations
- Contracts
- Internal reports
- Slack messages
- Email

Public
Documents intended for public consumption which can be freely distributed outside Tuist GmbH. Examples include:

- Marketing materials
- Product descriptions
- Release notes
- External facing policies

Labeling

Confidential data should be labeled "confidential" whenever paper copies are produced for distribution.

Data handling

Confidential Data Handling

Confidential data is subject to the following protection and handling requirements:

- Access for non-preapproved roles requires documented approval from the data owner
- Access is restricted to specific employees, roles and/or departments
- Confidential systems shall not allow unauthenticated or anonymous access
- Confidential Customer Data shall not be used or stored in non-production systems/environments
- Confidential data shall be encrypted at rest and in transit over public networks in accordance with the Cryptography Policy
- Mobile device hard drives containing confidential data, including laptops, shall be encrypted
- Mobile devices storing or accessing confidential data shall be protected by a log-on password (or equivalent, such as biometric) or passcode and shall be configured to lock the screen after five (5) minutes of non-use
- Backups shall be encrypted
- Confidential data shall not be stored on personal phones or devices or removable media including USB drives, CD's, or DVD's
- Paper records shall be labeled "confidential" and securely stored and disposed of in a secure, approved manner in accordance with data handling and destruction policies and procedures
- Hardcopy paper records shall only be created based on a business need and shall be avoided whenever possible
- Hard drives and mobile devices used to store confidential information must be securely wiped prior to disposal or physically destroyed
- Transfer of confidential data to people or entities outside the company shall only be done in accordance with a legal contract or arrangement, and the explicit written permission of management or the data owner

Restricted Data Handling

Restricted data is subject to the following protection and handling requirements:

- Access is restricted to users with a need-to-know based on business requirements
- Restricted systems shall not allow unauthenticated or anonymous access
- Transfer of restricted data to people or entities outside the company or authorized users shall require management approval and shall only be done in accordance with a legal contract or arrangement, or the permission of the data owner
- Paper records shall be securely stored and disposed of in a secure, approved manner in accordance with data handling and destruction policies and procedures
- Hard drives and mobile devices used to store restricted information must be securely wiped prior to disposal or physically destroyed

Public Data Handling

No special protection or handling controls are required for public data. Public data may be freely distributed.

Data retention

Tuist GmbH shall retain data as long as the company has a need for its use, or to meet regulatory or contractual requirements. Once data is no longer needed, it shall be securely disposed of or archived. Data owners, in consultation with legal counsel, may determine retention periods for their data.

Personally identifiable information (PII) shall be deleted or de-identified as soon as it no longer has a business use.

Retention periods shall be documented in the Data Retention Matrix in Appendix B to this policy.

Data & device disposal

Data classified as restricted or confidential shall be securely deleted when no longer needed. Tuist GmbH shall assess the data and disposal practices of third-party vendors in accordance with the Third-Party Management Policy. Only third-parties who meet Tuist GmbH requirements for secure data disposal shall be used for storage and processing of restricted or confidential data.

Tuist GmbH shall ensure that all restricted and confidential data is securely deleted from company devices prior to, or at the time of, disposal. Confidential and Restricted hardcopy materials shall be shredded or otherwise disposed of using a secure method.

Personally identifiable information (PII) shall be collected, used and retained only for as long as the company has a legitimate business purpose. PII shall be securely deleted and disposed of following contract termination in accordance with company policy, contractual commitments and all relevant laws and regulations. PII shall also be deleted in response to a verified request from a consumer or data subject, where the company does not have a legitimate business interest or other legal obligation to retain the data.

Annual data review

Management shall review data retention requirements during the annual review of this policy. Data shall be disposed of in accordance with this policy.

Legal requirements

Under certain circumstances, Tuist GmbH may become subject to legal proceedings requiring retention of data associated with legal holds, lawsuits, or other matters as stipulated by Tuist GmbH legal counsel. Such records and information are exempt from any other requirements specified within this Data Management Policy and are to be retained in accordance with requirements identified by the Legal department. All such holds and special retention requirements are subject to annual review with Tuist GmbH's legal counsel to evaluate continuing requirements and scope.

Policy compliance

Tuist GmbH will measure and verify compliance to this policy through various methods, including but not limited to, business tool reports, and both internal and external audits.

Exceptions

Requests for an exception to this Policy must be submitted to the IT Manager for approval.

Violations & enforcement

Any known violations of this policy should be reported to the IT Manager. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version history

Version	Date	Description	Author	Approver
1.0	Oct 23, 2024	Version 1.0	Pedro Piñera Buendía	Pedro Piñera Buendía

APPENDIX A - Internal retention and disposal procedure

Tuist GmbH's Engineering Team is responsible for setting and enforcing the data retention and disposal procedures for Tuist GmbH managed accounts and devices.

Customer Accounts:

1. Customer accounts and data shall be deleted within sixty (60) days of contract termination through manual data deletion processes.

Devices:

1. Employee devices will be collected promptly upon an employee's termination. Remote employees will be sent a shipping label and the return of their device shall be monitored.
2. Collected devices will be cleared to be re-provisioned - or removed from inventory, Tuist GmbH will securely erase the device when reprovisioning.
3. Device images may be retained at the discretion of management for business purposes

Destroying devices or electronic media
In cases where a device is damaged in a way that Tuist GmbH cannot access the Recovery Partition to erase the drive, Tuist GmbH may optionally decide to use an E-Waste service that includes data destruction with a certificate. Tuist GmbH will keep certificates of destruction on record for one year. Physical destruction can be optional if it is verified that the device is encrypted with Full Disk Encryption, which would negate the risk of data recovery.

Management will review this procedure at least annually.

APPENDIX B - Data retention matrix

System or Application	Data Description	Retention Period
Tuist GmbH SaaS Products	Customer Data	Up to 60 days after contract termination
Tuist GmbH Customer Sales (Attio)	Sales Data	Indefinite
Security Policies	Security Policies	1 year after archive