Data Management Policy

Policy Owner: Valentín Torassa Colombero

Effective Date: Jun 30, 2025

Purpose

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

Scope

All Teramot data, information and information systems.

General requirements

Teramot 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 Teramot 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 records
- Salary, compensation, and payroll data
- Strategic and product roadmaps
- Security incident and risk assessment reports
- Technical vulnerability reports
- Authentication credentials, secrets, and private keys
- Source code
- Legal and litigation data

Restricted
Teramot 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 and procedures
- Legal agreements and contracts
- Meeting minutes and internal presentations
- Internal reports and operational plans
- Slack messages and internal communications
- Emails and project documentation

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

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

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 by personnel not explicitly pre-approved requires documented approval from the data owner or executive leadership.
- Access is limited to authorized employees, roles, and departments with a demonstrated business need.
- Systems containing confidential data must not permit unauthenticated or anonymous access.
- Confidential customer data must not be used or stored in development, test, or other non-production environments.
- Confidential data must be encrypted at rest and in transit over public or untrusted networks, in accordance with the Cryptography Policy.
- Mobile devices, including laptops, that store confidential data must have encrypted storage.
- Mobile devices accessing confidential data must be protected by a secure log-on mechanism (e.g., password, passcode, or biometric) and must auto-lock after two (2) minutes of inactivity.
- Backups containing confidential data must be encrypted.
- Confidential data must not be stored on personal devices or removable media (e.g., USB drives, CDs, DVDs).
- Paper records containing confidential data must be clearly labeled "Confidential" and must be stored and destroyed securely, following the company's data handling and destruction procedures.
- Hardcopy paper records shall be created only when strictly necessary and avoided whenever possible.
- Hard drives and mobile devices that stored confidential data must be securely wiped before disposal or physically destroyed.
- Transmission of confidential data to external parties is only permitted with explicit written authorization from the data owner or management, and must occur under a legal agreement or contract.

Restricted Data Handling

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

- Access is limited to users with a legitimate business need and shall follow the principle of least privilege.
- Systems containing restricted data must not allow unauthenticated or anonymous access.
- Transfer of restricted data to external parties or unauthorized users must have prior management approval and must be done under legal agreement or data-sharing arrangement, or with explicit permission from the data owner.
- Paper records containing restricted data must be securely stored and destroyed following approved procedures.
- Devices that stored restricted data must be securely wiped or physically destroyed before disposal.

Public Data Handling

No special protections or handling requirements apply to public data.
Public data may be freely accessed, used, and distributed without restriction.

Data retention

Teramot 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. Teramot shall assess the data and disposal practices of third-party vendors in accordance with the Third-Party Management Policy. Only third-parties who meet Teramot requirements for secure data disposal shall be used for storage and processing of restricted or confidential data.

Teramot 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, Teramot may become subject to legal proceedings requiring retention of data associated with legal holds, lawsuits, or other matters as stipulated by Teramot 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 Teramot's legal counsel to evaluate continuing requirements and scope.

Policy compliance

Teramot 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 CEO for approval.

Violations & enforcement

Any known violations of this policy should be reported to the Cybersecurity Analyst. 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	Jun 30, 2025	Version 1.0	Valentín Torassa Colombero	Bruno Ruyu

APPENDIX A - Internal retention and disposal procedure

Teramot's Engineering Team is responsible for setting and enforcing the data retention and disposal procedures for Teramot 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, Teramot 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 Teramot cannot access the Recovery Partition to erase the drive, Teramot may optionally decide to use an E-Waste service that includes data destruction with a certificate. Teramot 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
Teramot SaaS Products (AWS)	Customer Data	Up to 60 days after contract termination
Teramot AutoSupport	Customer instance and metadata, debugging data	Indefinite
Teramot Customer Support Tickets	Support Tickets and Cases	Indefinite
Security Policies	Security Policies	1 year after archive
Temporary Files	AWS /tmp ephemeral storage	automatically when process finishes