pivot

Data Management Policy

Version: 1.0.0

Updated on: September 23, 2025

Purpose

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

Scope

All company data, information, and information systems.

Policy

The classification of data and information systems is done 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 employees and stakeholders easily understand requirements associated with different kinds of information, the company has created three classes of data.

Confidential

Highly sensitive data, or Confidential data, requires 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. Example include:

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

Restricted

Company proprietary information requires thorough protection; access is restricted to employees with a “need-to-know” based on business requirements. This data can only be distributed outside the company with approval. This is the 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 can be freely distributed outside the company. Examples include:

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

Labeling Paper

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 Security Delegate
- Access is granted on an as-needed basis.
- Access is restricted to specific employees, roles, and/or departments
- Confidential systems shall not allow unauthenticated or anonymous access
- Confidential Customer Data shall be handled like Company confidential data.
- 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 fifteen (15) minutes of non-use

- Backups of Confidential data shall be encrypted
- Confidential data shall not be stored on removable media including USB drives, CDs, or DVDs
- 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 of Confidential data 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 or as mandated by law or regulation, 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
- Restricted data shall not be stored on removable media including USB drives, CDs, or DVDs

Public Data Handling

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

Data Retention

Company 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 security leadership and/or legal counsel, may determine retention periods for their data.

Personally identifiable information (PII) shall be deleted or de-identified when 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. The organization shall assess the data and disposal practices of third-party vendors in accordance with the Third-Party Management Policy. Only third parties who meet company requirements for secure data disposal shall be used for the storage and processing of restricted or confidential data.

Where feasible, all restricted and confidential data will be 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, the organization may become subject to legal proceedings requiring retention of data associated with legal holds, lawsuits, or other matters as stipulated by 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 the company's legal counsel to evaluate continuing requirements and scope.

Policy Compliance

The company will measure and verify compliance with 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 Security Delegate for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Security Delegate. 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.

APPENDIX A – Internal Retention and Disposal Procedure

Engineering personnel are responsible for setting and enforcing the data retention and disposal procedures for company-managed accounts and devices.

Customer Accounts:

1. Customer accounts and data shall be deleted within ninety (90) days of contract termination and data no longer being needed for business purposes through manual data deletion processes.

Devices:

1. Employee devices will be collected promptly upon an employee's termination.
2. Remote employees will be sent a shipping label and the return of their device shall be monitored.
3. Collected devices will be cleared to be re-provisioned—or removed from inventory;
4. The company will securely erase the device when reprovisioning.
5. Device images may be retained at the discretion of management for business purposes.
6. The company may employ a third party to manage the above.

Destroying devices or electronic media

In cases where a device is damaged in a way that it cannot be accessed in order to erase the drive, the company may optionally decide to use an E-Waste service that includes data destruction with a certificate. Certificates of destruction will be kept 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.

APPENDIX B – Data Retention Matrix

System or Application	Data Description	Retention Period
Company SaaS Products	Customer Data	Up to 90 days after contract termination
Company Support	Customer instance and metadata, debugging data	Indefinite
Company Customer Support Tickets	Support Tickets and Cases	Indefinite
Company Customer Support Phone Conversations	Support Phone Conversations	Indefinite
Company Security Event Data	Security and system event and log data, network data flow logs	On-Premise - Indefinite Cloud/Host Instance - 1 year
Company Vulnerability Scan Data	Vulnerability scan results and detection data	6 months host (asset) data is retained until removed and purged from the vulnerability management tool
Company Customer Sales	Opportunity and Sales Data	Indefinite
Company QA and Testing Data	QA, testing scenarios, and results data	Indefinite
Security Policies	Security Policies	1 year after archive
Temporary Files	IaaS /tmp ephemeral storage	automatically when the process finishes

Document History

Version	Date	Description	Written by	Approved by
1.0.0	08/14/2025	Initial Version	Ryan Rich	Bishal Das