Data Management Policy

Policy Owner: VIMBuild, LLC
Author: Martin Ashton
Effective Date: 02/06/2025

Purpose

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

Scope

All VIMBuild, LLC data, information, and information systems.

Policy

VIMBuild, LLC 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 VIMBuild, LLC 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. 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

VIMBuild, LLC proprietary information requiring thorough protection; access is restricted to employees with a "need-to-know" based on business requirements. 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 VIMBuild, LLC. 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

- 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 devices storing or accessing confidential data shall be encrypted and protected by a log-on password or biometric authentication.
- Backups shall be encrypted.
- Confidential data shall not be stored on personal devices or removable media.
- Hard drives and mobile devices storing confidential information must be securely wiped prior to disposal.
- Transfer of confidential data to external entities must be authorized by management.

Restricted Data Handling

- Access is restricted to users with a need-to-know.
- Transfer of restricted data outside the company requires management approval.

- Paper records shall be securely stored and disposed of securely.
- Hard drives and mobile devices used for restricted information must be securely wiped before disposal.

Public Data Handling

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

Data Retention

VIMBuild, LLC shall retain data as long as it is needed for business, regulatory, or contractual requirements. Personally identifiable information (PII) shall be deleted or de-identified as soon as it is no longer needed.

Retention periods shall be documented in the Data Retention Matrix (Appendix B).

Data & Device Disposal

- Restricted or confidential data shall be securely deleted when no longer needed.
- Third-party vendors must meet VIMBuild, LLC's secure data disposal requirements.
- Confidential and restricted hardcopy materials shall be shredded or securely disposed of.
- PII shall be securely deleted in response to verified consumer requests unless legally required to retain it.

Annual Data Review

Management shall review data retention requirements annually. Data shall be disposed of according to this policy.

Legal Requirements

Certain legal proceedings may require data retention beyond normal policies. Such records shall be retained per legal counsel guidance.

Policy Compliance

VIMBuild, LLC will verify compliance through business tool reports, internal and external audits.

Exceptions

Requests for exceptions must be submitted to the Administrator for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the Administrator. Violations can result in suspension of system privileges and disciplinary action, including termination.

Appendix A - Internal Retention and Disposal Procedure

- Customer accounts and data shall be deleted within sixty (60) days of contract termination.
- Employee devices shall be collected and securely erased upon termination.

- Devices deemed unrecoverable shall be disposed of via an E-Waste service with data destruction certification.

Appendix B - Data Retention Matrix

System/Application	Data Description	Retention Period
VIMBuild SaaS Products	Customer Data	Up to 60 days after contract termination
VIMBuild Customer Support Tickets	Support Tickets and Cases	Indefinite
VIMBuild Security Event Data	Security and system logs	On-Premise - Indefinite, Azure - 1 year
VIMBuild Vulnerability Scan Data	Scan results	6 months
VIMBuild Sales Data	Opportunity and Sales Data	Indefinite
VIMBuild QA & Testing Data	Testing scenarios and results	Indefinite
Security Policies	Policy records	1 year after archive