RampedUp Document Retention and Destruction Policy

Data Destruction and Retention Policy

1. Purpose

The purpose of this **Data Destruction and Retention Policy** is to establish clear guidelines for the secure management, retention, and destruction of data within **RampedUp**. This policy ensures that data is retained for only as long as necessary, and destroyed securely when no longer required, in compliance with legal, regulatory, and contractual obligations.

2. Scope

This policy applies to all data generated, collected, stored, or processed by **RampedUp** in any format, whether digital, physical, or otherwise. It covers all employees, contractors, partners, and third-party vendors who handle company data.

3. Definitions

- **Data**: Any information, in any format, including but not limited to documents, files, databases, emails, and system logs.
- **Retention Period**: The period of time that data must be kept for legal, regulatory, or business purposes before it can be destroyed.
- **Destruction**: The process of securely and irreversibly rendering data unreadable or inaccessible.
- **Sensitive Data**: Personal, financial, or confidential information that requires special protection under laws, regulations, or industry standards (e.g., GDPR, HIPAA, PCI-DSS).
- **Backup Data**: Copies of data made for disaster recovery or business continuity purposes.

4. Data Retention

4.1. Retention Guidelines

RampedUp will retain data in accordance with legal, regulatory, and business requirements. Data retention periods will vary depending on the type of data, its purpose, and any applicable laws.

Data retention categories include:

- **Financial Data**: Retained for a minimum of 7 years after the conclusion of the fiscal year in which it was created.
- **Employee Records**: Retained for a minimum of 7 years after employment termination, unless otherwise required for tax or legal purposes.
- **Customer Data**: Retained for the duration of the business relationship, and for a period of 3 years after the last interaction or transaction, unless otherwise specified by law or contract.
- **Sensitive Data**: Retained only as long as necessary for business or legal purposes, and subject to periodic review to ensure its ongoing necessity.

- **Project Data**: Retained for 5 years after the project completion or as per client contract, whichever is longer.

4.2. Review and Documentation

At regular intervals, the Data Retention Team will conduct an internal audit to review the retention periods of all data categories. The review will ensure that data is not retained beyond its required period and to evaluate compliance with applicable regulations. Documentation will be kept for all retention decisions and audits.

5. Data Destruction

5.1. Destruction Process

Data that is no longer needed will be destroyed in a manner that renders it irretrievable. Destruction methods will vary depending on the type and format of the data:

- **Digital Data**:
  - **Hard Drives and Storage Devices**: Data will be destroyed using industry-standard data wiping software that meets or exceeds the standards specified in NIST SP 800-88 (Guidelines for Media Sanitization).
  - **Cloud Data**: Data stored on cloud platforms will be destroyed by utilizing platform-specific secure deletion protocols or encryption key destruction.
  - **Backup Data**: All backup copies will be securely overwritten or destroyed when they are no longer needed.
- **Physical Data**:
  - **Paper Documents**: Shredding will be used to destroy paper documents containing sensitive or confidential information. Shredders must meet at least a P-4 security level.
  - **Physical Media**: CD/DVDs, USB drives, and other removable media will be physically destroyed or shredded.

5.2. Destruction Process for Sensitive Data

When dealing with sensitive data (e.g., personal identifying information, payment card data), additional measures will be taken to ensure compliance with applicable privacy laws and standards. Destruction of sensitive data will be verified and documented by the Information Security team, and certified destruction services will be used when applicable.

5.3. Third-Party Data Destruction

When data is entrusted to a third-party vendor for processing or storage, the company will ensure that the vendor has an established, enforceable data destruction policy in place. Any third-party vendors handling sensitive data must provide evidence of compliance with this policy.

6. Data Backup and Archival

6.1. Backup Data Retention

Backup data will be retained in accordance with the same retention periods as regular operational data, unless otherwise required by business or disaster recovery needs. All backup data will be securely stored and access will be restricted to authorized personnel only.

6.2. Archival Data

Data required for long-term storage due to regulatory requirements or business needs will be archived. Archives must be securely encrypted and access will be controlled. Archive data will be reviewed periodically to assess if it is still required.

7. Roles and Responsibilities

7.1. Data Retention Team

The Data Retention Team is responsible for overseeing the implementation of this policy, ensuring that data is retained for appropriate periods, and ensuring the proper destruction of data when it is no longer needed. The team will also document retention decisions and destruction actions for audit purposes.

7.2. Information Security Team

The Information Security Team will ensure that all data destruction processes follow best practices for security and compliance. This team will also provide periodic training on data destruction methods and tools, and ensure that data is irreversibly destroyed.

7.3. Employees

Employees are required to adhere to this policy and notify the Data Retention Team if they are unsure of data retention or destruction requirements. Employees must follow the secure destruction procedures for physical and digital data when disposing of company data.

8. Compliance and Legal Requirements

8.1. Applicable Laws

This policy complies with all applicable data privacy laws, including but not limited to:

- **General Data Protection Regulation (GDPR)**
- **Health Insurance Portability and Accountability Act (HIPAA)**
- **Payment Card Industry Data Security Standard (PCI-DSS)**
- **Federal and state data retention laws**

8.2. Legal Holds

In the event of litigation or government investigation, a legal hold may be placed on specific data. A legal hold suspends the destruction or deletion of data related to the legal matter, and it will remain in place until authorized by the Legal Team.

9. Training and Awareness

9.1. Employee Training

All employees, contractors, and third-party vendors who handle company data will receive regular training on data retention and destruction procedures. The training will cover the importance of secure data destruction and the legal consequences of non-compliance.

9.2. Ongoing Awareness

RampedUp will maintain an ongoing awareness program to remind employees about their responsibilities regarding data destruction and retention. This will include periodic updates and refreshers on the policy.

10. Monitoring and Audits

10.1. Internal Audits

Regular internal audits will be conducted to verify compliance with this policy. These audits will include reviewing data retention periods, destruction processes, and any exceptions.

10.2. Compliance Audits

Third-party audits may be conducted to verify compliance with relevant regulations, including data protection laws.

11. Policy Violations and Consequences

Any employee found violating this policy may face disciplinary action, up to and including termination. Serious violations, particularly those resulting in data breaches, may also lead to legal action or penalties.

12. Policy Review and Updates

This policy will be reviewed annually or as necessary to ensure that it remains compliant with all applicable laws, regulations, and business needs. Any updates to this policy will be communicated to all employees and stakeholders.