BoostUp.ai
Data Retention, Archival and Destruction Policy

Last updated: Jan 3rd, 2019

What is Data/Record Retention?

The **retention** period of data and/or a document is an aspect of records information management. It represents the period of time a document should be kept or "retained" both electronically and in paper format. It describes (1) length of time each document or record will be retained as an active record, (2) reason (legal, fiscal, historical) for its retention, and (3) final disposition (archival or destruction) of the record.

Policy

Active, inactive, and historical records must be maintained in accordance with the Record Retention Schedule and this Policy. Expired records are reviewed first and destroyed based on management approval in accordance with this Policy.

Data Retention, Archival and Destruction Policy requires BoostUp's personnel to:

1) Retain important records for reference and future use;
2) Delete or destroy records that are no longer necessary for the proper functioning of the organization;
3) Suspend record destruction upon notice from BoostUp.ai Legal;
4) Provide BoostUp.ai Departments with the ability to organize records for efficient retrieval; and
5) Know what records should be retained, the length of their retention, means of storage and when/how they should be destroyed.

The Record Retention Schedule designates the custodian/department for each type of record.

This Policy covers all records and documents, including electronic documents, contains guidelines for how long certain documents should be kept and how records should be destroyed. The Policy is designed to promote compliance with federal and state laws and regulations, to minimize accidental or innocent destruction of records

Purpose

BoostUp.ai recognizes that it is good business practice to retain records in a consistent, systematic, and reliable manner so that they can be retrieved promptly when required for legal, regulatory, or operational reasons.

This Policy has been developed to provide guidance and direction to BoostUp.ai employees on how to:

- Manage internal Company Records throughout their lifecycle and clarify responsibilities, according to sound business and legal practices.

- Establish data/records retention program
- Set archival procedures
- Prepare proper destruction of data files

Confidentiality Statement

At BoostUp.ai, we are committed to responsible data management, which includes the use, protection and destruction of customer and company confidential information.

Responsibility of Those Granted Access to Customer and Corporate Data and Records
Employees and business partners who have been granted access to any informational assets are accountable for its protection, use, disclosure and destruction. It is their responsibility to protect the assets against loss, and unauthorized access, modification or disclosure.

Responsibility of Management
BoostUp.ai Senior Management is responsible for identifying and establishing the most appropriate protection and retention of data and associated records. Management must be guided by the law and by internal corporate policies and procedures in authorizing access, use, retention and destruction of these data assets, electronic and paper.

It is also management's responsibility to ensure that employees understand their responsibilities regarding the proper retention, archival and destruction of data and associated records.

Responsibility & Scope

The Chief Technology Officer (CTO) has the primary responsibility for the implementation and monitoring of the internal compliance policy, related security policies, standards and practices and recordkeeping for **BoostUp.ai** and owns the technology underpinning the development and production environments and works with the internal team to ensure that key security standards are met and that a robust technology plans are in-place.

This Policy will apply to:

- All individuals defined as employees, contractors, consultants and/or temporary personnel working for or on behalf of **BoostUp.ai;**
- All third-party partners and vendors working with **BoostUp.ai;**
- Any information processed by production systems (financial, corporate, customer and personal);
- **BoostUp.ai** corporate and production systems; and
- The ability to protect, detect and take actions against threats to **BoostUp.ai** systems.

Data Retention Procedures

Ingested Customer data (e.g. SaaS-app usage metrics) is retained for a timeframe per requirements/agreements per customer. All such data is deleted from our systems as required per customer agreements or when requested by the customer. This does not include customer communication (e.g. emails, slack messages).

- Customers must request this by emailing support@boostUp.ai
- We delete the customer data from our primary datastores within 30 business days of a customer request. We notify the customers of the data-deletion via email.
- We delete the customer data from our data backups within 60 business days of a customer request.
- If requested by the customer, we will delete all records containing PII for a specific employee, within the timeframe listed above.
- If requested by the customer, we will stop ingesting all future records containing PII for a specific employee, within the timeframe listed above.

BoostUp.ai retention, archival and destruction procedures include:

Initial Notifications

- CTO is to be notified, prior to any action, about any destruction request.
- Engineering will handle ONLY electronic material. The individual groups will destroy physical records as necessary.
- Engineering will complete the request in the timeframe listed above.

Input the Request into Ticketing System

- If a request is received through JIRA, the ticket is assigned to Engineering.
- If a request is received by Email, a subsequent email is to be submitted on behalf of the sender to JIRA, so that a ticket is created. The ticket is assigned to Engineering.
- Any email received outside of JIRA by Desktop Support staff should be added to the JIRA ticket and forwarded to Engineering.

Proof of Request

To obtain proof of the destruction request, the following information is needed.

- The physical email/letter/memo received by the Account Management team from the client (preferred) needs to be included in the JIRA ticket.
- A note, included in the JIRA ticket, from the Account Manager indicating that the request was received verbally from the client.

Deletion of the Electronic Data Records

After the notifications and requests and have been completed and documented, the designated electronic data record(s) is deleted from the production and archived locations.

- Engineering personnel performs the deletion/purge of electronic records.

Notification of Destruction

The notification of destruction should be recorded in the JIRA ticket.

- Attached screenshots of the removal of Virtual Machines (VMs) and/or data folders.
- Notify customer of deletion/purge of data records within 30 days.

Who Should Read and Understand This Policy

This policy should be read by:

<u>BoostUp.ai Management:</u>

- To ensure that data retention, archival and destruction requirements are properly addressed and updated.

<u>BoostUp.ai Teams</u>

- To ensure retention and destruction are consistently implemented and followed.

Enforcement & Exceptions

BoostUp.ai reserves the right to temporarily or permanently suspend, block, or restrict access to information assets when is reasonably appears necessary to do so to protect the confidentiality, integrity, availability, or functionality of those assets.

If it is determined that there is non-compliance with or a violation of this policy, the employee(s) or contracted individual(s) may be subject to immediate disciplinary action, up to and including termination.

Policy Management

This policy will be reviewed, at least annually, by the author or designated CTO or designee and updated as necessary to properly address current business needs.