Data Backup Policy

Version number	2.0
Last Approved	Feb 25, 2025
Classification	PUBLIC

Overview

The Data Backup Policy provides minimal guidance on the retention, duration and the backup and restoration methodologies used to securely store copies of systems in a manner that protects the privacy of data and the integrity of copies of the SaaS hosting infrastructure and client data. These guidelines meet industry best practices and ensures The Company retains ‘safe’ immutable backup copies to prevent data loss due to physical destruction or retroactive modification. The disposition of backup media is covered by the Data Retention, Destruction and Disposal Policy.

Applicability

The applicability of this statement falls under purview of the Security Documentation Overview.

Purpose

This policy defines the retention timelines for backup storage of The Company’s system images, customer data stored within, and other related SaaS infrastructure needed to operate The Company’s systems. Guidelines applicable to both physical and cloud infrastructure ensure that backups (on whatever media or storage device) are retained in a secure manner to prevent loss due to physical destruction and accidental or intentional modification of the data by online means.

Backup images shall be retained for a period of time to allow multiple restoration points to mitigate loss from accidental or intentional modification of system data such that a copy of data can easily be recovered with readily available tools - even data from files that were deleted long

ago or a hard drive that was reformatted. Given the evolving nature of ransomware methodologies, simply having a prior copy is insufficient as it may also be tainted. Data must be retained in an offline or immutable/versioned manner with sufficient restoration points allowing restoration to multiple earlier points.

Failure to properly backup and restore data may result in the loss of The Company's and customer's data and could result in the loss of software license keys, breach of SLA objectives and/or result in fiscal penalties.

Scope

This policy applies to any electronic information storage and physical media containing sensitive or confidential data stored within The Company's hosted facilities or trusted subcontractors maintaining offsite or immutable online copies of systems and customer data. This applies to all media including, but not limited to: disk drives, CDs, DVDs, magnetic tape, removable drives, memory cards and sticks, USB drives, and any other devices with persistent storage, both online or offline.

Data Backup Policy

Backup Strategy

The Company's services have been built with Confidentiality, Integrity, and Availability in mind. When practical and possible, real-time replication to multiple locations provides an initial level of data backup. Additionally, instance in time backups shall be taken to ensure immutable restoration points.

Backups include all OS, utilities, security and other software, and data files necessary for recovery. If applicable, a plan to identify replacement hardware used for backups shall be part of the recovery plan. Data encryption practices require that encryption keys are replicated and/or stored offsite using a different backup methodology.

Backups shall be stored in diverse physical locations (ideally at least 10 miles from the original data) within each region and are encrypted.

The Company must regularly perform restoration tests to ensure that data is correctly restored and that backups are valid. The test objective may be met by either a 'needed' restore in the course of business, or if no opportunity is present, a random selection of data restored as a validation test.

The Company performs Disaster Recovery tests for each backup methodology utilized (cloud account, datacenter facility for each region) at least once per year and implements a model of

continual improvement for environments. See Business Continuity Planning and Disaster Recovery Policy for more information on DR.

SOC 2: A1.2

The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

Frequency and Storage

The Company shall perform a scheduled/automated backup of customer data and encryption key systems at least once a day.

This policy does not specify the location nor method of backup, so long as it meets certain requirements:

- Backups must not be stored in the same location as the original data for more than 7 days (eg: tape library) but may be immediately replicated offsite (e.g: a cloud based backup system)
- Backups must be immutable copies not subject to modification once taken, regardless of storage location, until such time as the backup policy is set to “delete” the data.
- Backups shall be encrypted (data at rest) with sufficient safeguards on encryption keys as specified in our Encryption Key Management Policy.
- Remote storage of backups must be held in a secure location subject to adherence of our Physical Security Policy.

Backups shall be audited to ensure both successful and failure cases are properly reporting and data is able be restored as part of a backup restoration test.

Backup Retention Periods

- **Daily** Backups shall be retained for 31 days (required).
- **Weekly** Backups are retained for 6 months (recommended).
- **Monthly** Backups are retained for 1 year (recommended).

Backups shall not be maintained longer than 13 months from the date of backup execution.

Data Retention & Media Disposal

Refer to Data Retention, Destruction and Disposal Policy for further information on Data Retention.

Additional Information

Additional information related to *Disciplinary Actions*, *Exceptions* and *Questions* can be found in the Security Documentation Overview.

Document control

This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Art Machado	
Author(s)	@Art Machado @angelina.kilmer @Paul Gordon	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Feb 25, 2025
Review cycle	ANNUAL	
Next review date	Feb 24, 2026	

Version History

Date	Author(s)	Version	Changes
Feb 25, 2025	@Art Machado @angelina.kilmer @Paul Gordon	2.0	Annual review
Nov 4, 2024	@Art Machado	1.8	Frequency and storage requirement update
Nov 01, 2024	@angelina.kilmer	1.7	Changed Policy classification from Confidential to Public
Oct 28, 2024	@Art Machado @Paul	1.6	Update to retention periods

	Gordon @angelina.kilmer		
Mar 13, 2024	@Art Machado , @Sarah Zwicker (Unlicensed) , @Paul Gordon	1.5	Annual review, minor updated to language
Jul 25, 2023	@John Cole	1.4	Updated Strategy to include physical storage considerations
Feb 23, 2023	@Art Machado , @Sarah Zwicker (Unlicensed)	1.3	Annual review + logo updated
May 18, 2022	@John Cole , @Sarah Zwicker (Unlicensed)	1.2	Updated Strategy, Frequency and Storage
Apr 14, 2022	@Sarah Zwicker (Unlicensed)	1.1	Initial Review and Approval
Mar 31, 2022	@Art Machado , @Sarah Zwicker (Unlicensed)	1.0	Original version