Data Retention Policy

[Company Name]

Purpose

This policy outlines the requirements and controls/procedures [COMPANY NAME] has implemented to manage the retention and deletion of customer data.

Policy

For Customers

Customer data is retained for as long as the account is in active status. Data enters an “expired” state when the account is voluntarily closed. Expired account data will be retained for **<X days>**. After this period, the account and related data will be removed. Customers who wish to voluntarily close their account should download their data manually or via the API prior to closing their account.

If a customer account is involuntarily suspended, then there is a **<X day>** grace period during which the account will be inaccessible but can be reopened if the customer meets their payment obligations and resolves any terms of service violations.

If a customer wishes to manually back up their data in a suspended account, then they must ensure that their account is brought back to good standing so that the user interface will be available for their use. After **<X days>**, the suspended account will be closed and the data will enter the “expired” state. It will be permanently removed **<X days>** thereafter (except when required by law to retain).

Secure Disposal or Reused of Equipment

Before disposal or reuse, [COMPANY NAME] will verify that all equipment containing storage media has been purged of any sensitive data and licensed software. This data will either be securely overwritten or entirely removed.

If a cloud service customer, [COMPANY NAME] is responsible for obtaining assurances from cloud service providers that they have established policies and procedures for the secure disposal or reuse of resources. Cloud service providers engaged by [COMPANY NAME] must ensure that measures are in place for the secure and prompt disposal or reuse of resources, including but not limited to equipment, data storage, files, and memory.

Protection of Records

All records within [COMPANY NAME] will be shielded from loss, destruction, falsification, and unauthorized access or release in alignment with legislative, regulatory, contractual, and business obligations.

If a cloud service customer, [COMPANY NAME] will solicit information from its cloud service provider regarding the security measures in place for the protection of records collected and stored in the cloud that are pertinent to [COMPANY NAME]’s utilization of cloud services. Cloud service providers utilized by [COMPANY NAME] must disclose information about the safeguarding measures for records they gather and store that relate to [COMPANY NAME]’s use of their cloud services.