**Purpose and Scope**

This Data Retention and Disposal Policy addresses how a customer's data is retained and disposed of and ensures this is done consistently. From time to time, [Organization Name] may update this policy. This policy is guided by security requirements specific to [Organization Name] including compliance with applicable laws and regulations.

This policy applies to all [Organization Name] assets utilized by personnel acting on behalf of [Organization Name] or accessing its applications, infrastructure, systems, or data. All personnel are required to read, accept, and follow all [Organization Name] policies and plans.

**Data Retention**

The time period for which [Organization Name] must retain customer data depends on the purpose for which it is used. [Organization Name] must retain customer data for as long as an account is active or in accordance with the agreement(s) between [Organization Name] and the customer, unless [Organization Name] is required by law or regulation to dispose of data earlier or retain data longer.

**Data Disposal**

[Organization Name] must dispose of customer data within 30 days of a request by a current or former customer or in accordance with the Customer’s agreement(s) with [Organization Name]. [Organization Name] may retain and use data necessary for the contract such as proof of contract in order to comply with its legal obligations, resolve disputes, and enforce agreements. [Organization Name] hosting and service providers are responsible for ensuring the removal of data from disks allocated to [Organization Name] use before they are repurposed and the destruction of decommissioned hardware.

Only a limited number of [Organization Name] employees shall have access to delete customer data.

Upon employee or contractor termination, company-owned devices will be collected and sanitized prior to device re-issuance in accordance with NIST Guidelines for Media Sanitization (NIST S.P. 800-88 Rev. 1).