

Data Retention and Disposal Policy

Status: Published, [Secureframe Link](#)

Published date: May 11, 2026

Last updated: May 11, 2026

Policy owner: Daniel Imfeld

Purpose and Scope

This Data Retention and Disposal Policy addresses how a customer's data is retained and disposed of and to ensure this is carried out in a consistent manner. From time to time, Deviceflow may update this policy. This policy is guided by security requirements specific to Deviceflow including compliance with applicable laws and regulations.

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

Data Retention

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

Data Disposal

Deviceflow 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 Deviceflow. Deviceflow 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. Deviceflow hosting and service providers are responsible for ensuring the removal of data from disks allocated to Deviceflow use before they are repurposed and the destruction of decommissioned hardware.

Only a limited number of Deviceflow employees should 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).

Exceptions

Deviceflow business needs, local situations, laws and regulations may occasionally call for an exception to this policy or any other Deviceflow policy. If an exception is needed, Deviceflow management will determine an acceptable alternative approach.

Enforcement

Any violation of this policy or any other Deviceflow policy or procedure may result in disciplinary action, up to and including termination of employment. Deviceflow reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Deviceflow does not consider conduct in violation of this policy to be within an employee's or contractor's course and scope of work.

Any employee or contractor who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of Deviceflow as soon as possible.

The disciplinary process should also be used as a deterrent to prevent employees and contractors from violating organizational security policies and procedures, and any other security breaches.

Responsibility, Review, and Audit

Deviceflow reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually.

This document is maintained by Daniel Imfeld.

This document was last updated on May 11, 2026.

Attestation

I attest that the information provided in this document is accurate and complete to the best of my knowledge.

Field	Value
Name	Anatoly Geyfman
Title	CEO
Signature	
Date	07/29/2026