Title: Dell Media Sanitization Statement	**Issue Date:** 27 November 2024
Document Number: RQD0302	**Revision Number**: 2.1

Media Sanitization of Data Storage Devices

Dell understands and shares Dell Customers' concerns regarding the security of data. Dell has implemented media sanitization practices to help control data security risk for data storage devices returned to Dell and for services carried out at a Customer's location. Dell implements these processes throughout its return streams and with Dell's suppliers to operationalize the practices described in this statement.

Customers that are subject to legal or regulatory obligations regarding sanitization of media, and Customers that have other heightened data security or privacy concerns or risk factors, should do one of the following:

1. ensure that data has been removed, encrypted or properly sanitized prior to returning their data storage device to Dell (with appropriate measures taken to comply with any applicable legal or regulatory obligations);

2. purchase "Keep Your Hard Drive for Client/Keep Your Components for Client" or "Keep Your Hard Drive for Enterprise/Keep Your Components for Enterprise" service from Dell; or

3. purchase or otherwise arrange for a sanitization/destruction process or service before the unit(s) leave their control. Dell can provide sanitization/destruction services, including services at a Customer's location, such as Dell's "Asset Recovery Services" and "Data Sanitization and Data Destruction for Infrastructure Services".

Sanitization

For all data storage devices returned to Dell and for services carried out at a Customer's location, unless Customers contract with Dell to perform a Dell sanitization/destruction service with a higher security standard applicable to the Customers' specific devices or components, Dell's approach to the handling of data storage devices is to either:

1. sanitize the device (in alignment with the IEEE 2883 or US Department of Commerce NIST SP 800-88 Rv. 1 "Purge" or "Clear" methods) in preparation for reuse;

2. when Dell elects not to reuse the device or when it is pre-sorted for recycling Dell will initially destroy the device using physical crushing, shredding or other appropriate physical destruction method (in preparation for recycling, and in accordance with the IEEE 2883 "Destruct" method or US Department of Commerce NIST SP 800-88 Rv. 1 "Destroy").

Neither Dell nor Dell's suppliers access any customer data as part of screening, sanitization, testing, refurbishment, or unit repair. Dell has processes and controls for the physical safeguarding of all material

passing through Dell's physical control in Dell's return streams. Dell performs regular audits of its own facilities and operations, as well as its partners and suppliers who are authorized to perform data security processes regarding physical security and sanitization.

Customer advice

Dell advises customers to always secure, backup and or remove any data stored on a device as applicable before returning it to Dell. Pursuant to the applicable warranty or support services contract, Dell is under no contractual obligation to perform a sanitization on any returned device(s) and assumes no liability for any data left on these devices per the terms of those agreements. Customers should not attempt to disable or physically destroy a data storage device, in any manner (e.g., degaussing, shredding, drilling, etc.) before returning it to Dell. Damaging devices that a customer is obligated to return pursuant to the terms of the applicable warranty and service contract the customer purchased with the applicable device will result in charges for any devices damaged or not returned to Dell.

Revisions

Date	Description
November 2024	Minor updates
October 2023	Revised to align with IEEE 2883
October 2022	Minor updates
April 2022	Service offerings updated
March 2019	Reviewed
June 2017	Initial publication

Dell   One Dell Way, Round Rock, Texas 78682   512.338.4400   **Dell.com**