

Laptop & desktop sanitisation for the enterprise

Organisations must effectively sanitise data on IT assets, including laptops and desktops (both Mac and PC), before redeployment, tech refresh, resale, return, or recycling. Maintaining a secure chain of custody is crucial for a compliant audit and reporting process. We provide help with both.

Our certified data sanitisation platform, Teraware™, operates at scale, wiping data across your IT assets, from fleets of devices to different asset types located in multiple locations.

We offer sanitisation options designed to match your security settings, goals, and requirements across departments, locations, or regions.

Common use cases

- › High volume in-house user equipment processing
- › Low volume in-house processing of multiple user computers
- › Individual user computer or server processing

Deployment

- › Teraware can be deployed to meet specific use cases with deployment options including
 - › Server appliance
 - › USB
 - › Custom hardware
- › Additional charges for Teraware hardware
- › Optional support package available

Licensing

- › Licenses are assigned to the server appliance or USB unique to the client
- › License quantities are sold in predetermined volumes based on use case
- › Custom license volumes and hardware solutions quoted on a per client basis

Compliant with industry standards

Iron Mountain recognises the National Institute of Standards and Technology (NIST) 800-88 as an ideal framework for device sanitisation.

Certifications

Forensic audit certified by ADISA Certification Limited, Threat Matrix Level 2, for both SSDs and HDDs, Teraware delivers on providing security, speed, and scalability. Its rapid and comprehensive solution makes it the most efficient data sanitisation choice worldwide for data centres and end-user devices, regardless of the challenge or volume of assets.

NIST

ADISA®

Customised sanitisation options to match your security goals and requirements

