IDSC International Data Sanitization Consortium

Proper / Improper Data Sanitization

PROPER

Physical Destruction

The process of shredding hard drives, smartphones, printers, laptops and other storage media into tiny pieces.

Cryptographic Erasure (Crypto Erase)

The process of using encryption software (either built-in or deployed) on the entire data storage device, and erasing the key used to decrypt the data.

Data Erasure

The software-based method of securely overwriting data from any data storage device using zeros and ones onto all sectors of the device.

IMPROPER

Data Deletion

The act of hiding data on a storage device, whereby the data is available for overwrite. Until the data has been overwritten, the data is still easily recoverable.

Reformatting

Reformatting is performed on a working disk drive to eliminate its contents. By formatting, it leaves most, and sometimes all, existing data on the storage device.

Factory Reset

A factory reset removes all user data and restores a device back to factory settings, providing the device is not rooted.

Data Wiping

The process of overwriting data, without verification that the overwriting was successful in overwriting all sectors of the storage device, and does not produce a certified report.

File Shredding

File Shredding destroys data on individual files and folders by overwriting the space with a random pattern of 1's and 0's.

Data Clearing

Data Clearing protects against keyboard attacks and applies to logical techniques to sanitize data in all user-addressable storage locations for protection against simple, non-invasive data recovery techniques.

Data Purging

Data Purging protects against laboratory attacks and applies to physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.

Data Destruction

Data Destruction is destroying data from digital storage media so that it is completely unreadable and cannot be accessed or used for unauthorized purposes.