ISO 27000 Data Sanitization Requirements

"ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS), though there are more than a dozen standards in the ISO/IEC 27000 family. Using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties."

Data Sanitization to Protect the Data on Devices

Practicing effective data sanitization is essential in assuring that no data on a device is ever recovered, whether it is unintentional or without authorization.

Read about Secure Equipment and Media Disposal According to ISO 27001 here.

The International Data Sanitization Consortium says that "Data Sanitization is the process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable. A device that has been sanitized has no usable residual data, and even with the assistance of advanced forensic tools, the data will not ever be recovered. There are three methods to achieve data sanitization: physical destruction, cryptographic erasure, and data erasure."

Although data destruction and data sanitization have similarities in their approach, they are not the same. Data destruction does not include verification or certification of successful destruction beyond forensic recovery. This means that the chosen data destruction method has not been proven to remove data in totality, whether that target is a single file or an entire drive.

Visit www.clarabyte.com to read our eBook on Data Sanitization Best Practices.

ISO 27000	
SPECIFICATION	**DATA SANITIZATION SIMPLIFICATION**
A.11.2 Equipment **A.11.2.7 Secure Disposal or Reuse of Equipment Control** All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Destroy all data with a proven data sanitization method regardless of the information stored on the device.

Remove all data with Clarabyte

Clarabyte's intuitive and flexible data erasure software allows highly-regulated organizations to easily automate their data sanitization processes to improve security, eliminate the risk of human error when processing devices, and guarantee compliance with ISO 27000 or any of the most strict data protection regulations. Clarabyte's proprietary algorithm offers data erasure for the entire spectrum of hard drives and solid-state drives, with verification of successful erasure, and tamper-proof reporting. This unmatched level of control over data removal eliminates the risk that data will ever be recovered so that devices may be securely reused, sold, or donated. No other data sanitization method is able to compare in risk elimination, scalability, or automation.

Click here to learn more about ClaraWipe Pro.

References:

https://www.iso.org/isoiec-27001-information-security.html