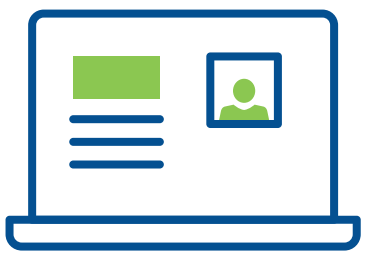
IDSC International Data Sanitization Consortium

7 Benefits of Implementing a Data Sanitization Policy

To minimize your organization's risk exposure against data breaches, you must first map your data across each stage of its lifecycle (create, store, use, share, archive and destroy). To achieve the final step-destroy-implement data sanitization methods that make data permanently unrecoverable through physical or digital means. Here are seven benefits you'll get from implementing data sanitization across your organization.

1



Achieve Data Hygiene and Data Retention Best Practices

Data erasure for files/folders is part of overall data maintenance, ensuring that redundant data isn't stored unnecessarily, which can increase IT costs and the risks of data loss/theft and data breaches. Data retention policies should be mapped against data sanitization processes at the end of the retention period to prevent losing control of managed data.

2

Avoid Data Spillage

Data spillage occurs when information in any form is moved from a protected system and introduced into a system that does not give it the same or better level of protection as the system from which it was moved.

During this time, sensitive data can be inadvertently copied. That data should not just be deleted, but permanently and verifiably erased.

3

Securely Handle Confidential Files

When an employee receives and handles confidential data on a PC temporarily, that data should be securely erased from the system without delay to prevent potential data leaks. Make this policy a reality by automating recycle bin erasure on a regular basis. More granular polices to securely erase specific file types by revision number and time stamp should also be implemented.

4

Safeguard Data Migration

Whenever data is moved from one location to another—from a retired server to a new server, or from one virtual machine to another—the original data location must be erased. Erasure is necessary for LUN reuse in a hosted environment when a user migrates to a larger LUN or leaves the cloud so that the LUN can be safely reassigned to a new user. This is true for both physical servers using LUNs as storage and for virtual machines with dedicated storage on a LUN to comply with ISO 27018.

5

Protect End-of-Life, Classified Virtual Machines

Virtual machines (VMs) are often used for short-term projects. When these projects are completed, the data on these machines must be securely erased. Targeted erasure of a VM is necessary when the VM is deleted or changes location in the data center. Organizations should be able to achieve this without rebooting the host. By installing the erasure solution at the VMware ESXi level, organizations can manually erase VMs in VMware vSphere. All files associated with the targeted VMs should be erased, including VMDK, VMSD, VMX and VMXF.

6

Meet Customer Demand

Data sanitization is necessary for B2B partners who wish to terminate their relationship and require a data erasure audit trail after the end of their contracts. Many NDAs stipulate this.

Additionally, in jurisdictions such as the EU, the EU GDPR's "right to be forgotten" rules dictate that consumers may ask to have their data removed from company servers and organizations must comply. It's not enough to simply delete customer records. Instead, records must be completely expunged without any possibility of recovery. An audit trail with a certified report proves that the erasure occurred.

7

Protect Temporary Data

During major disasters, data is typically recovered at an offsite location. The same is true during disaster-recovery exercises, where real customer data is typically used. It's critical to erase this data from the secondary site. Once production systems are restored, any data left on recovery disks should be also erased. Additionally, this could apply to "test exercises" when real data is being used.

For more information on creating a data sanitization policy, read the *7 Steps to Create a Data Sanitization Policy* eBook.