



# 7 Steps to Create a Data Sanitization Policy

---

August 2017

# Introduction




---

Securely disposing of data is more difficult than you might think. The National Institute of Standards and Testing (NIST) outlines seven steps to creating an overarching cyber security framework. These steps are also applicable to creating a comprehensive [data sanitization](#) process to destroy, erase or remove data from any IT asset, at any organization. Put them into practice to reduce risk, lessen the impact of a cyber security attack and stay compliant with data protection and privacy regulations.

## What is the correct definition of data sanitization?

It's 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 never be recovered.

There are three methods to achieve data sanitization:

-  Physical Destruction
-  Cryptographic Erasure
-  Data Erasure

# Step 1: Prioritize and Scope.

---

First, your organization must recognize the risks associated with lack of control over information throughout its lifecycle and the need for an information lifecycle approach that entails proper data sanitization processes across each step. Identify information stores and applications within the scope of this policy, and dedicate resources to data sanitization as it is implemented. Work with your highest priority information first.

Once you've identified the risks, create a checklist that lists the types of information that will need to be considered. This data audit will encompass all types of data that are collected, stored, processed, archived and disposed of.

This information may include:

- Employee records (healthcare, performance, disciplinary actions, financial)
- Personally identifiable information (PII)
- Customer records
- Email and other corporate communications
- Legal documents (contracts, MOUs, public filings)
- Transaction/sales records
- Intellectual property (patents, notes, research records)
- Marketing material
- Customer support documentation
- Manufacturing quality documentation

Once you determine the types of information you have, you must break down which applications are storing these records. These could fall within multiple categories depending on redundancy of systems. These types of applications include:

- Databases
- Microsoft applications, such as Excel, Word, PowerPoint, etc.
- Cloud-Based systems (either on-premise or hosted through a third-party provider)
- Back-up drives
- CRM systems
- Endpoint/employee PCs/laptops

After mapping the applications in which each of the information types are stored, you must map the primary business line owner/department who is responsible for the information and the functions that create the information.

Eliminate data types, applications and regions you may not be addressing.



## Step 2: Orient.

Once the scope of your data sanitization program has been determined, identify regulatory requirements and overall data exposure risks. Then detect threats to, and vulnerabilities of, data stores, systems and assets used to process that data.

During this step, it is important to:

- a. Understand the data that is subject to regulatory requirements.
- b. Understand the risk exposure of the data from each of the category types and applications/systems. Risk exposure is dependent on the sensitivity of the data and the accessibility/security of the storage device itself.
- c. Prioritize the risk exposure based on the type of data and the storage device (level of 1 – 10, with 1 being highest risk exposure and 10 being the lowest exposure to risk).

[Click here](#) for a list of regulatory requirements and standards regarding data sanitization.

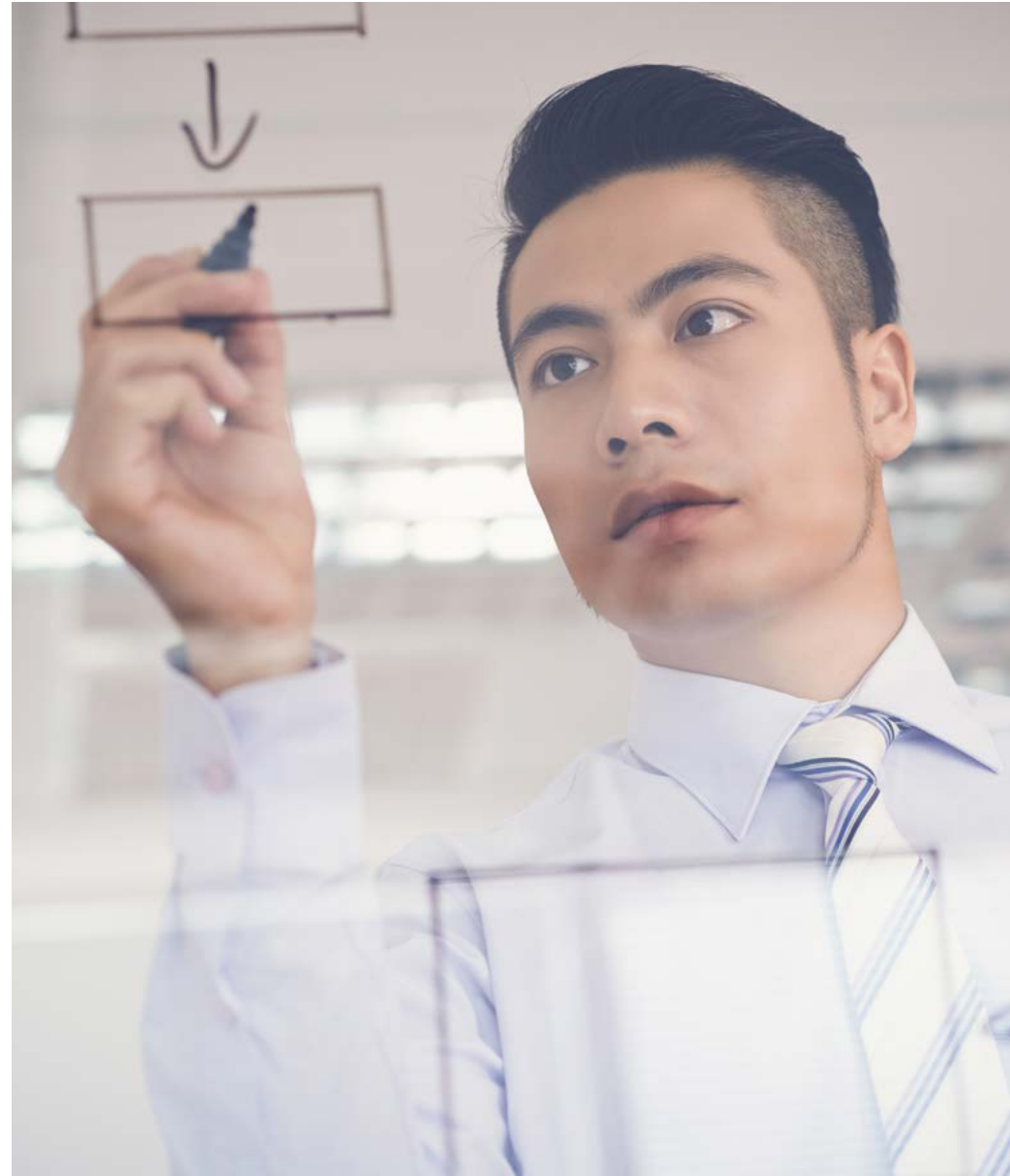


## Step 3: Create a Current Profile.

Next, create a flowchart of the existing information processes within your organization with supporting documentation. Understand when and where the information is created, who creates it and when it moves through each phase of the lifecycle. Determine, where required, the appropriate method of data sanitization.

- a. Map each of the processes across the lifecycle. Include where, if at all, data sanitization practices are present.
- b. Understand the data sanitization method(s) currently being used and how these methods are being carried out. For most companies, there are two points when data sanitization should occur – 1) when the data storage device reaches end-of-life and 2) when the data reaches end-of-life (i.e. no longer needed or required by the organization).

For example, end-of-life should map the process by which new customers are onboarded and how records are created and maintained as your orders are fulfilled, delivered, invoiced and payments received. You should ask the following questions. As the records age, how are they archived? For how long? Is there a record retention policy for each regulatory environment? What is the appropriate procedure for disposing of those records at the end of their life?



## Step 4: Conduct a Risk Assessment.

---

Identify the risk of regulatory action, including fines and oversight, imposed by regulators based on the current state of data protection in your organization. Then quantify potential risks to your organization from improperly disposing of data. This may include loss of IP, breach notification costs and impact on brand and customer satisfaction.

- a. Determine which processes are subject to the greatest regulatory risk (rating 1 – 10).
- b. Assess the possibility of a data breach across each process (rating 1 – 10).
- c. Quantify the impact of a data breach and/or non-compliance across each process (use calculator).
- d. Based on a-c, develop a prioritized list of those with the greatest impact and risk to your organization.



## Step 5: Create a Target Profile.

---

After selection of the prioritized list of those business processes, including types of data and storage devices with the greatest impact of risk, your organization can now establish goals for managing data sanitization.

The target profile is the desired end state. This is a fully implemented data sanitization program. For each prioritized business process and class of information, you must define its end of life (retention period) and appropriate data sanitization method. For each process, map out the future state of where, when and how data sanitization should occur.





## Step 6: Determine, Analyze and Prioritize Gaps.

Determine what technologies, processes and people are required to move from your current state to the target profile mentioned previously. Here are two examples of data sanitization gaps many companies face:

1. **There is no process in place for permanently sanitizing temporary files.**  
In this case, a plan should be put in place to deploy client software, using routines from the IT Administrator group deployed through Microsoft Active Directory. This will allow for automatic sanitization of these temporary files on a daily basis, reducing your overall risk of exposure to data loss/theft.
2. **You return data center assets back to the manufacturer for warranty with information still left on them.** Prior to returning the drive(s), a full disk erasure process must be deployed.





## Step 7: Implement an Action Plan.

---

To close these gaps and continuously improve data sanitization practices across every department in your organization, you'll need an action plan. Create measurable milestones and revisit your data sanitization strategy annually.

Ready for the next step? Download our editable [Data Erasure Policies & Procedures for IT Assets](#) and [General Requirements for Full Data Sanitization Implementation](#) policy templates to begin building and executing your organization's data sanitization policies.

