**About This Document**

This companion piece to our [Data Erasure Policies & Procedures for IT Assets](http://www.datasanitization.org/wp-content/uploads/2017/08/data-erasure-policies-procedures-for-it-assets.docx) policy document provides guidance on working with data sanitization partners and suppliers and suggestions for policy ownership and auditing, including responsibilities for managing data sanitization across multiple roles in the organization. Customize this editable template to fit your organization’s goals.

**Procedure for Partners and Suppliers**

Units should make sure data sanitization procedures are also adopted by subcontractors, suppliers or partners that handle part of COMPANY’s data.

When implementing these requirements, management is also recommended to exercise due diligence of the other party. Due diligence for this case could include:

* Reviewing an independent audit of the company’s operations and/or its compliance with this document
* Reviewing and evaluating the disposal company’s information security policies or procedures
* Taking other appropriate measures to determine the competency and integrity of the potential information management in the company

**Audit trail requirement**

The following minimum requirements should be met for software performing data erasure.

The data erasure software must be documented to state the successful completion of the process and must include:

1. Equipment or data media serial number or erasure target name or path
2. The erasure standard used
3. A tamper-proof certificate that the erasure has been done correctly
4. A reliable system for managing audit trails in high volume and over time

**Policy ownership**

Best practice dictates that the CIO or CISO delegates the ownership of this data erasure policy to the internal IT security team.

Tasks include:

1. Ownership of the policy document
2. Coordination of suppliers
3. Overseeing updates of internal existing statements of work including data sanitization processes and enabling internal and external audit processes.

Each operational team identified as a process or asset owner in this policy should have documented work flows and responsibilities.

**Mandatory Revisions**

This document does not claim to cover all possible technical equipment or data media that COMPANY could possibly use to store or process data. Yearly revisions are recommended to update the policy.

**Governance**

**Roles and Responsibilities**

**CEO**The Chief Executive Officer must recognize the requirement for a data sanitization policy and provide for the resources required to implement it. The CEO should review the scope and gap analysis and approve the implementation of the action plan.

**Risk Committee**

The risk committee should identify the risks from both compliance infractions and data loss arising from improperly disposing of assets and data. It should ensure that controls are in place to reduce these risks through data sanitization and the implementation of this policy.

**Board**

The board of directors should ask for periodic updates and ensure that the corporate risk committee is part of the process.

**Chief Information Governance Officer (CIGO)**

The CIGO, Chief Privacy Officer, Chief Data Officer and/or the Data Protection Officer should be responsible for creating, publishing, and maintaining the data sanitization policy. This role will establish a budget and ensure resources are deployed to achieve compliance with this policy.

**Chief Information Security Officer**

The CISO will approve this policy and ensure that it is incorporated in the enterprise security strategy for data protection. This role will also oversee third party compliance with the data sanitization policy for suppliers, partners and outsourced security services.

**Data Architects**

Data architects and DBAs will participate in creating the controls to identify data at risk and ensure the mechanisms are in place to apply data sanitization procedures when called for by this policy.

**For more information about creating a data sanitization policy across your organization,** [**contac­t us**](mailto:info@datasanitization.org)**­ today.**