Building a data sanitization policy and implementing and enforcing it throughout your organization is a complicated task. Use the following template to ensure all unnecessary or end-of-life data is disposed of securely across all IT assets. Customize the fields to fit your organization’s goals.

**IT Assets & End-of-Life Destruction**

Technical equipment that must be thoroughly sanitized before resale, reuse or recycling includes:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PCs | Laptops | Tablets | Servers | Storage Systems |
| Photocopier | Network Printer | Network Fax | Routers | Switches |
| Firewalls | Proxy Filters | Network Attached Storage (NAS) | Point-of-Sale Equipment (POS) | Barcode Readers |
| Smartphones | Removable Memory Devices (USB, etc.) | Loose Drives (from any of the above) |  |  |

Examples of Data Media:

|  |
| --- |
| CD |
| DVD |
| Back-up Tape |

This rule applies to the following, non-exhaustive, situations:

|  |  |  |
| --- | --- | --- |
| End-of–life disposal | Re-deployment within the organization; Staff leaving or being reassigned | Maintenance work outside of the organization’s premises |
| End-of-lease return of equipment | Warranty claims / RMA returns | Service claims |

**Asset Lifecycle Procedures/ Policies**

Asset lifecycle procedures are developed to ensure digital data is adequately protected from unauthorized disclosure when technical equipment or data media is being redeployed within THE COMPANY, disposed of (end-of-life) or in any other way is leaving THE COMPANY’s, or a third-party partner´s, physical control. The latter can include off-site service, for example, or Returned Material Authorization (RMA) from the manufacturer.

This type of equipment contains data, sometimes being proprietary, classified, company confidential, personal or otherwise of a sensitive nature, as well as software that carries license restrictions.

Before a change of control may take place, all technical equipment capable of storing or processing company data must use data erasure. This can be completed within the organization’s IT department, or a selected partner can facilitate the process during the change of control. These selected partners include leasing companies that own the equipment, outsourcing partners that own and / or manage the equipment or a professional ITAD (IT Asset Disposal company) that is contracted for its services.

With these security measures in place, the goal of the policy is to improve organizational procedures for encouraging reuse of equipment within the organization or by new users outside the organization. Company policy should be enacted to minimize impact on the environment from equipment extending its life through reuse,

donation or parts usage. The following facts from a UN report are examples of information behind this policy and viewpoint:

* A computer’s energy use is dominated by production (81%), as opposed to operation (19%).
* Computer manufacturing is energy intensive: the ratio of fossil fuel use to product weight is 11-1.
* 1.8 tons of material are used to manufacture a desktop PC and monitor.

**Suggested Process: Overview**

All technical equipment capable of storing or processing company data must use data erasure by a certified and approved data erasure software vendor before change of control may take place. The process should allow for full documentation and traceability so for example an individual hard drive can be proven to be erased properly if questioned. This follows ISO27001 recommendations.

**Example Contract Language for a Third Party**

Pro-customer:

1. **RETURN OR DESTRUCTION OF CONFIDENTIAL INFORMATION**

1.1 For the purpose of this Clause, (a) “Confidential Information” means all confidential information (including, but not limited to, the information related to operations, processes, product, know-how, technical information, designs, trade secrets, personal data, financial information, business affairs, market opportunities etc.) relating to the purpose which the Customer directly or indirectly discloses, or makes available, to the Supplier.

1.2 If so requested by the Customer at any time by notice in writing to the Supplier, or upon the termination of the agreement, the Supplier shall promptly: (a) destroy or return to the Customer all documents and materials (and any copies) containing, reflecting, incorporating or based on the Customer’s Confidential Information; (b) permanently erase all the Confidential Information from its computer and communication systems and devices used by it, or which is stored in electronic form, and to the extent technically and legally practicable, from the systems and data storage services (including cloud platforms) provided by third parties; and (c) provide the Customer with a digitally signed, tamper-proof certificate of proof of secure erasure from a certified data erasure software solution in the market, or from a reputed data erasure service provider certified by the Common Criteria and other security organizations worldwide.

1.3 Supplier may retain any documents and materials containing or based on the Confidential Information that the Supplier is required to retain by applicable law, or to satisfy the requirements of a regulatory authority or body of competent jurisdiction or the rules of any listing authority or stock exchange, to which it is subject. Confidentiality obligations shall continue to apply to any documents and materials retained by the Supplier pursuant to this Clause. At the end of the legal retention period, the Supplier shall destroy the physical copies of the Confidential Information and permanently erase all the Confidential Information stored in electronic form and provide the certificate of erasure to the Customer as required above.

1.4 The obligations herein shall survive the termination of the agreement and shall remain in full force and effect.

Mutual:

1. **RETURN OR DESTRUCTION OF CONFIDENTIAL INFORMATION**

1.1 For the purpose of this Clause, (a) “Confidential Information” means all confidential information (including, but not limited to, the information related to operations, processes, product, know-how, technical information, designs, trade secrets, personal data, financial information, business affairs, market opportunities etc) relating to the purpose which the Discloser directly or indirectly discloses, or makes available, to the Recipient; (b) “Discloser” means the party that discloses its Confidential Information, directly or indirectly, to the Recipient; and (c) “Recipient” means the party that receives Confidential Information, directly or indirectly, from the Discloser.

1.2 If so requested by the Discloser at any time by notice in writing to the Recipient, or upon the termination of the agreement, the Recipient shall promptly: (a) destroy or return to the Discloser all documents and materials (and any copies) containing, reflecting, incorporating or based on the Discloser’s Confidential Information; (b) permanently erase all the Confidential Information from its computer and communication systems and devices used by it, or which is stored in electronic form, and to the extent technically and legally practicable, from the systems and data storage services (including cloud platforms) provided by third parties; and (c) provide the Discloser with a digitally signed, tamper-proof certificate of proof of secure erasure from a certified data erasure software solution in the market, or from a reputed data erasure service provider certified by the Common Criteria and other security organizations worldwide.

1.3 Recipient may retain any documents and materials containing or based on the Confidential Information that the Recipient is required to retain by applicable law, or to satisfy the requirements of a regulatory authority or body of competent jurisdiction or the rules of any listing authority or stock exchange, to which it is subject. Confidentiality obligations shall continue to apply to any documents and materials retained by the Recipient pursuant to this Clause. At the end of the legal retention period, the Recipient shall destroy the physical copies of the Confidential Information and permanently erase all the Confidential Information stored in electronic form and provide the certificate of erasure to the Discloser as required above.

1.4 The obligations herein shall survive the termination of the agreement and shall remain in full force and effect.

The requirement for data erasure of equipment not owned by the company must be covered by a legal contract with the equipment provider. Equipment or data media that *cannot* be securely erased may require physical destruction.

More details for implementation of this policy are available below for reference purposes.

**Data Erasure Procedures**

**Responsibility**

The process owner is responsible for validating that the result of the data erasure procedures meet the requirements set out in this document. Validation of data erasure procedures should occur annually, at a minimum, or whenever new technical equipment type or data media type is introduced. The validation process (see below) should be documented.

If a service provider is contracted to perform the data erasure procedure, full traceability should be required, and validation of this work must be done by organizations on an annual basis, if not more frequently.

As the process owner, external regulations or legislation may require specific procedures to be developed within a business process. Examples of this could be PCI DSS requirements (safekeeping credit card Information) and data protection legislation (prevention of unauthorized transfer or processing of personal data).

**Validation of Data Erasure Software and Equipment**

All data erasure procedures should be validated to meet the requirements stated in this document. Validation should rely on external certifications and approvals of software and equipment used for data sanitization. External certification and approval authorities should be organizations such as government certification authorities, national defense organizations and those authorized to perform tests and grant approvals for Common Criteria. Internal tests based on thorough analysis of erased media are also approved, if thoroughly documented and performed to meet industry standards.

Damaged storage devices or data media should be subject to a risk assessment to determine whether they should be destroyed, repaired or discarded.

Data erasure used on technical equipment or data media needs to be logged for future reference to maintain an audit trail.

In the case of leased technical equipment, the legal contract must cover these data erasure requirements.

Factors to be considered:

* Does a validated data erasure procedure exist for the specific type of equipment or media involved?
* Is the equipment or data media defective and data erasure prohibited?

In general, at the time when data changes location, there is a change of owner control of the device or the device leaves the organization’s premises, there will be a need for data erasure.

* **Personal Computers / PCs**For most PCs (laptops or desktops), it is not necessary to physically destroy hard drives if they have successfully passed the data erasure process. A PC has successfully executed data erasure if the procedure used has verifiably removed data from all addressable parts of the storage device.

Redundant PCs that are being disposed of, sold or donated should complete data erasure to this standard before leaving THE COMPANY’s control.
* **Servers and Server Storage Systems**Servers and server storage systems hold large volumes of data from a variety of sources. A separate data erasure procedure must be implemented for each type of storage system (e.g. NAS, SAN) and hard drive technology (e.g. RAID level, SCSI, ATA, SATA) in use. Data erasure can take place on a drive level or logical level (LUN-level).

**NOTE**: For loose drives, data erasure is necessary for sanitizing disks outside the host. This also applies to loose drives from storage area networks (SANs). Because of the chain-of-custody concerns, local data erasure of disks is necessary. Erasing loose drives requires an external host/boot device and connectivity between the drives and the host. Data erasure on failed disks removes the content so the drive can be transported to the OEM for warranty replacement. The data center, not the OEM, is responsible for data erasure.
* **Photocopiers, Network Printers and Fax Machines**Photocopiers are typically networked, with many of these machines doubling as network printers. Any photocopier, network printer or fax machine that contains a hard drive is likely to hold sensitive data. While this information is not readily available to end users of the machines, it is potentially available to maintenance staff. All such machines must therefore undergo data erasure procedures before they leave THE COMPANY for maintenance, disposal or replacement. Any removal or replacement of the hard drive must be controlled and the procedures properly adhered to. These devices should use data erasure when being re-purposed within THE COMPANY to prevent data from being exposed inter-department.
* **Mobile Phones / Smartphones/ Tablets**All mobile phones (cell phones) may potentially contain sensitive information that needs to be securely erased before change of control takes place, especially models with advanced level of functionality (e.g. smartphones). Where business communication is likely to have taken place, mobile phones must always use data erasure procedures. For mobile phones with SIM cards, all SIM cards must be removed before disposal and have data erasure performed on all memory cards that may reside in the unit.
* **Point-of-Sale (POS) Equipment**In many cases POS-equipment is leased, and the requirements of data erasure should be addressed in

a legal contract. If owned by THE COMPANY, similar procedures as used for personal computers or servers should be used.

* **Virtual Machines**When a virtual architecture takes advantage of elastic computing (expanding compute resources on demand) a process should be in place to ensure that no data is left behind when a VM is decommissioned, especially in public clouds.
* **Removable Solid State Memory Devices (e.g. USB Flash Drive, SD Card)**When using removable memory devices, deleted files can be recovered. Files on SD cards that have been re-formatted using Microsoft Windows Format function, for example, or the card's file system has been corrupted, may be recovered. Software overwrites that overcome the inherent protections of SSD memory should be used. Each device should then be tested to ensure the data sanitization occurred and a record kept.
* **CD / DVD / Optical Disk**The only approved solution to achieve data sanitization on CDs, DVDs or other type of Optical Disks is physical destruction.
* **Backup Tape**The only approved solution to achieve data sanitization on backup tapes or other types of magnetic tape media is physical destruction or degaussing.

**Out of Retention Period Data**

Files and data that have fallen outside of specific data retention periods, as dictated by the data retention policy, should be securely overwritten and a record created of the data sanitization action.

**For more information about creating a data sanitization policy across your organization,** **contac­t us****­ today.**