



Thank you for your interest in this Tabernus

WHITE PAPER

Establishing a Data Destruction Policy

*Things to Consider When Developing
Information Security Policies for
Your Business*

Executive Summary

This white paper is a high level set of recommendations for developing and instituting an end of lifecycle data destruction policy for a company of public sector agency. It covers three major topics:

- Things to consider when developing a company wide policy for data destruction.
- Educating the staff on the policy and the importance of data destruction.
- Documentation and certification of what is done during the process.

Introduction

Most businesses and public sector agencies understand that they are legally obligated to securely erase sensitive customer data at end of life for an electronic storage device. Yet many still do not have company wide policies which their employees are expected to follow. This is both irresponsible and potentially disastrous. With no policy in place, electronic media can “slip through the cracks” and sensitive data can be exposed.

There are three major areas to consider when creating a company policy for data destruction. They are:

- Establishing a thorough set of standards and processes which will be followed.
- Educating the staff about these policies.
- Documenting (electronically) everything that is done.

Each of these is detailed below.

Establishing a Data Destruction Policy

The first step is to determine a company policy for electronic data elimination. In most cases, there will

be different approaches used based on the equipment needing its sanitization, or the sensitivity of the data on this equipment.

When determining a company wide policy to follow, first evaluate everything in your business that may need data sanitization. Examples include:

- Hard drives in employee laptops and desktops
- Servers on the company LAN
- Storage devices/towers in the company data center
- Portable media (phones, USB drives, etc.)

A method of data destruction should be chosen for each circumstance that requires such data elimination. It is unlikely that each of the erasure scenarios listed above will utilize the same process. As an example, hard disk drives coming from storage towers are extremely expensive to replace, so physical destruction may not be ideal. USB thumb drives are easy and cheap to replace, so physical destruction may be a great option for them.

There are several key things to consider when determining a data elimination method for a certain type of electronic media:

- Can the device be reused or sold in the secondary market?
- Can the device be erased in a non-destructive method?
- Do you have a lease agreement on this equipment that will force you to pay penalties for media that is not returned at end of lease?

Educating the Staff on the New Data Destruction Policy

As with any policy, it is only strong if it is followed. Step one is to make sure the staff is aware of the policies set up and knows how to follow them. Make sure that the

staff understands the data erasing method that should be used for each piece of electronic storage media you own or lease.

It is also critical to make the staff aware of potential security breaches, such as a PCI breach, that they may not have considered. Examples of these include:

- USB drives
- Printers
- Copy machines
- Fax machines
- Portable hard drives
- Laptop, portable, or tablet computers

All of these devices have potentially sensitive data contained on them. Yet many of these devices are transported outside of the company walls daily. Educating the staff that these items do contain sensitive data will not only change their daily approach to protecting these devices, but will remind them that action must be taken at end of life for each device.

Documenting Data Elimination

While most companies and agencies understand the importance of eliminating electronic data at end of life, many still marginalize the necessary records keeping. Electronic records certifying all erasures should be maintained (and, depending on the industry, must be maintained). This electronic record should include at least the following information:

- Date of erasure
- Type of device erased
- Serial number of hard drive or storage devices erased
- Method used to erase the device

For future auditing purposes, it is also critical that this information be maintained in a format that does not allow for manipulation by a user. Non-editable PDF documents should be used in the place of editable spread sheets or other electronic files.

Tabernus, LLC

11130 Jollyville Road, Suite 301
Austin, Texas 78759
1.888.700.8560 (phone)
1.512.372.9790 (fax)
www.tabernus.com