Secure Disposal of Sensitive Data

1.0 Overview

Secure Disposal of sensitive data is essential to data protection and security. Destroying data means it can no longer be read by an operating system or application. Merely deleting a file is insufficient. Any loss of data due to improper data destruction is a liability. Furthermore, loss of data can severely impact the success of a project and client information. Requirements for effective data destruction can have different legal requirements concerning destroying data.

2.0 Purpose

The purpose of this plan is to provide a successful procedure for secure disposal of sensitive data from storage media due to increased scrutiny, as legal and ethical obligations make it more important than ever to protect data such as Personally Identifiable Information (PII).

3.0 Scope

These procedures apply to Information Technology Operators. The secure disposal of sensitive data includes, but is not limited to, these methods as applicable Delete/Reformat, Wipe, Overwriting data, Erasure, Degaussing, Physical destruction (drill/band/crush/hammer), Electronic shredding, Solid state shredding.

4.0 Procedures

DBAN Darik's Boot And Nuke (DBAN) is an entirely free data destruction program used to completely erase all the files on a hard drive.

Refer to Lifewire “How to Erase a Hard Drive using DBAN”

https://www.lifewire.com/how-to-erase-a-hard-drive-using-dban-2619148