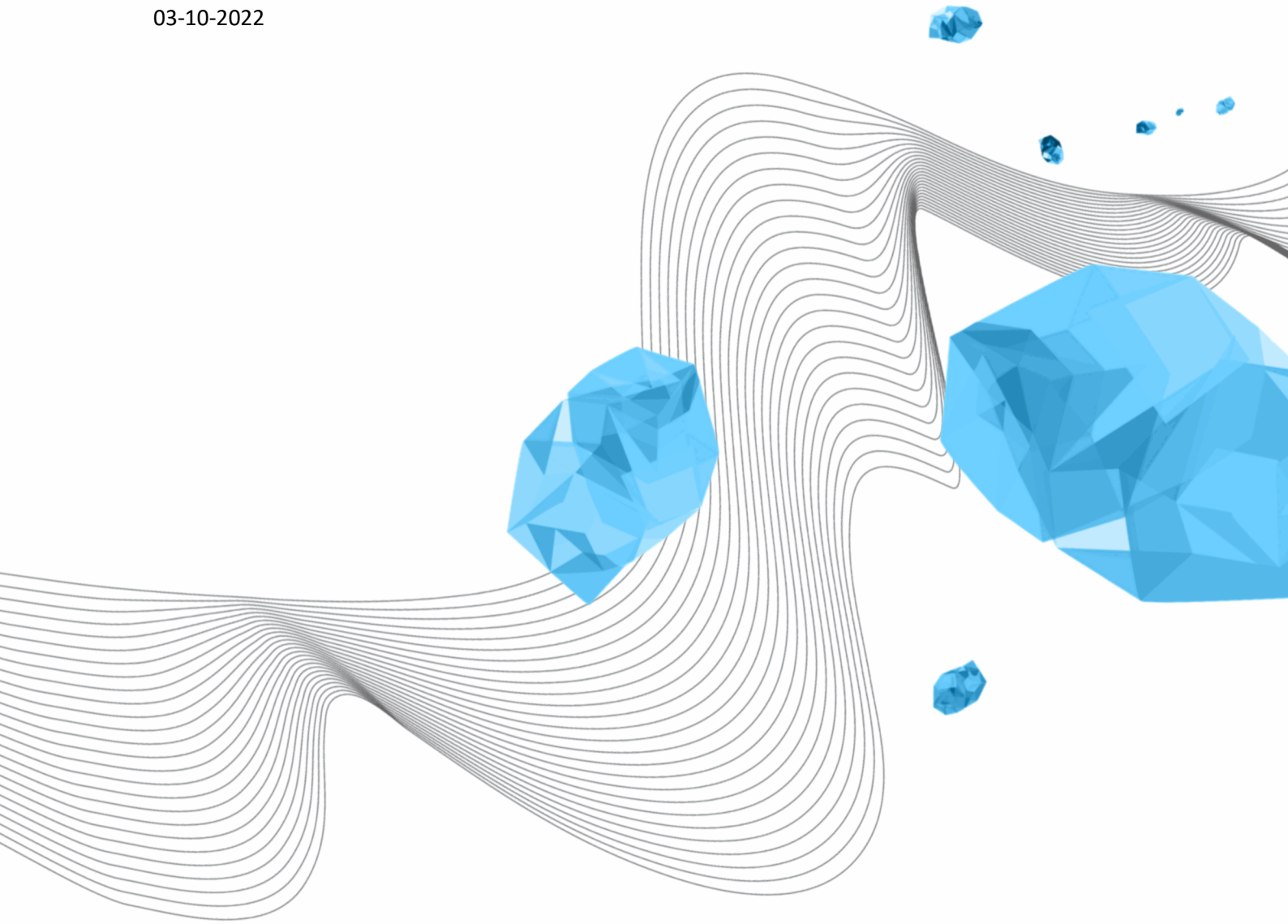
GUIDELINES ON DESTRUCTION OF DATA CARRIERS

[SUBJECT]

Peter Peters

Version 1.0

03-10-2022



UNIVERSITY OF TWENTE.

COLOPHON

ORGANISATION
Library, ICT Services & Archive (LISA)

TITLE
Guidelines on Destruction of Data Carriers

VERSION (STATUS)
1.0

DATE
03-10-2022

AUTHOR(S)
Peter Peters

DOCUMENT HISTORY

VERSION	DATE	AUTHOR(S)	REMARKS
0.1	25-2-2022	Peter Peters	First concept.
0.2	22-6-2022	Peter Peters	Update after consultation with LISA-ITO
0.3	28-9-2022	Peter Peters	Corrected several grammatical errors.
1.0	3-10-2022	Peter Peters	Final version for publication

DISTRIBUTION LIST

VERSION	DATE	DISTRIBUTED TO
0.1	25-2-2022	LISA security management
0.2	22-6-2022	LISA security management; selected team leaders ITO and CS
0.3	28-9-2022	LISA security management
1.0	3-10-2022	Cyber Safety Website

CONTENT

1 Introduction 4
2 Basic guidelines 4
2.1 Disposal 4
2.2 Reuse 4
3 Specific guidelines 5
3.1 Servers 5
3.2 Workstations 5
3.3 (Smart) phones 5
3.4 Other data carriers 5

1 INTRODUCTION

The Information Security Policy of the University of Twente has a security rule about the destruction of data carriers. This rule describes the process in general.

When data carriers such as hard discs, tapes, mobile devices, USB sticks etc. are put out of operation or disposed of, the data on them must be adequately destroyed by or on behalf of the owner.

This document describes the guidelines that should be followed for different kinds of data carriers as the ways to dispose of changes with the type of data and the kind of device.

These guidelines SHALL be followed in case there is even a slight change the data carrier containing sensitive material, either personal data governed by the GDPR[1] or other sensitive data.

Remember, data carriers can be in the strangest devices[2]. If the device has some way of storing data, it most certainly contains one or more data contains.

2 BASIC GUIDELINES

2.1 DISPOSAL

The University has contracted SUEZ to dispose of all waste. Part of this waste disposal is the regular removal, in a secure way, and destruction of sensitive information on paper.

SUEZ also offers ways to remove and dispose of digital data carriers. More information can be obtained from Campus & Facility Management[3].

2.2 REUSE

Reusing data carriers is only allowed if it is possible to wipe the data on the carrier completely. Otherwise, a data carrier SHALL NOT be reused.

Hard Disk Drives (HDD) can be wiped safely and securely. LISA advises the use of KillDisk[4] from LSoft Technologies Inc.

KillDisk SHALL NOT be used to erase data on Solid-State Disks (SSD).[5]

When a data carrier is wiped, KillDisk will present the user with a certificate stating the erasure method. The certificate SHALL be attached to the data carrier. When the data carrier is reused, the new user CAN remove the certificate.

USB disks, either thumb drives or external SSDs or HDDs, SHALL NOT be reused and SHALL be destroyed instead.

[1] General Data Protection Regulation; https://gdpr.eu/
[2] For instance Multi-functional Printers/Copiers store prints and scans on internal data carriers.
[3] https://www.utwente.nl/en/service-portal/services/cfm/maintenance/sorting-waste-materials
[4] https://www.killdisk.com/eraser.html
[5] An exception is made when the disk is a SATA drive directly connected to a computer running the Linux Operating System. In this case *Secure Erase* can be used to securely erase all data.

3 SPECIFIC GUIDELINES

3.1 SERVERS

Servers[6] usually contain one or more HDDs or SSDs.

When a server is decommissioned, the data carriers should be handled according to the basic guidelines (chapter 2).

For servers maintained by LISA, destruction of all data carriers by shredding in a professional shredder[7] is the default. This is to conform to ISO 27001 and NEN 7510 certifications.

LISA keeps a log of all disks disposed of by either means.

3.2 WORKSTATIONS

A user can request to buy his personal workstation. If they get permission, they SHALL present the workstation to LISA Servicedesk ICT. Included data carriers SHALL be wiped and prepared for reuse according to chapter 2.2.

3.3 (SMART) PHONES

Only smartphones with full encryption SHALL be reused. Refer to the manufacturer's manual or the Operating System manual for ways to wipe all data from the phone safely.

All other phones SHALL be disposed of safely and environmentally friendly.

Phones SHALL NOT be shredded or, in other ways, mechanically destroyed. The battery can cause fire and explosions.

3.4 OTHER DATA CARRIERS

Other data carriers, not previously mentioned, SHALL be disposed of safely and environmentally friendly.

[6] For the purpose of these guidelines Network Attached Storage and Storage Area Network systems are considered servers.
[7] https://satrindtech.com/en/