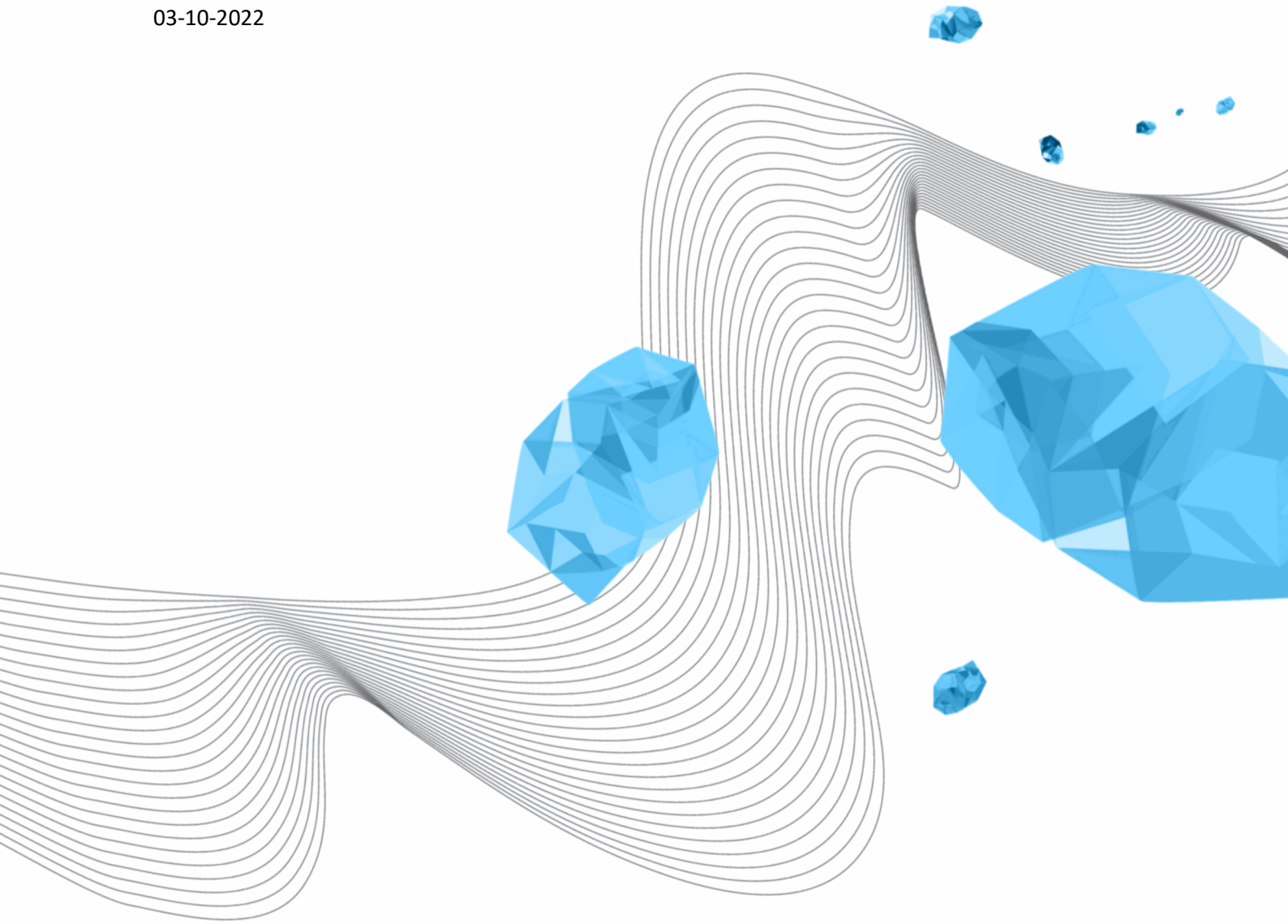
# RICHTLIJNEN VOOR HET VERNIETIGEN VAN DATADRAGERS

[SUBJECT]

Peter Peters

Versie 1.0

03-10-2022



# COLOFON

ORGANISATIE
Library, ICT Services & Archive (LISA)

TITEL
Richtlijnen voor het vernietigen van datadragers

VERSIE (STATUS)
1.0

DATUM
03-10-2022

AUTEUR(S)
Peter Peters



# DOCUMENTHISTORIE

| VERSIE | DATUM | AUTEUR(S) | OPMERKINGEN |
|---|---|---|---|
| 0.3 | 1-10-2022 | Peter Peters | Vertaald vanuit de Engelse versie 0.3 |
| 1.0 | 3-10-2022 | Peter Peters | Definitieve versie voor publicatie |
| | | | |

# DISTRIBUTIELIJST

| VERSIE | DATUM | AUTEUR(S) | GEDISTRIBUEERD AAN |
|---|---|---|---|
| 0.3 | 30-09-2022 | Peter Peters | LISA communicatie |
| 1.0 | 3-10-2022 | Peter Peters | Cybersafety website |
| | | | |

# INHOUDSOPGAVE

# 1 INLEIDING

Het Informatiebeveiligingsbeleid van de Universiteit Twente kent een beveiligingsregel over het vernietigen van gegevensdragers. Deze regel beschrijft het proces in het algemeen.

Wanneer gegevensdragers zoals harde schijven, tapes, mobiele apparaten, USB-sticks etc. buiten gebruik worden gesteld of worden verwijderd, dienen de gegevens daarop door of namens de eigenaar adequaat te worden vernietigd.

Dit document beschrijft de richtlijnen die moeten worden gevolgd voor verschillende soorten gegevensdragers. De richtlijnen wijzigen aan de hand van het type gegevens en het soort apparaat.

Deze richtlijnen MOETEN worden gevolgd in het geval er zelfs maar een kleine wijziging is in het gebruik van een gegevensdrager die gevoelig materiaal bevat, hetzij persoonsgegevens die onder de AVG[1] vallen, hetzij andere gevoelige gegevens.

Bedenk dat gegevensdragers in de vreemdste apparaten[2] kunnen zitten. Als het apparaat een manier heeft om gegevens op te slaan, bevat het zeker een of meer gegevensdragers.

# 2 BASIS RICHTLIJNEN

## 2.1 VERNIETIGING

De Universiteit heeft een contract met SUEZ voor de verwijdering van alle afval. Onderdeel van die afvalverwijdering is het, op een veilige wijze, verwijderen en vernietigen van gevoelige informatie op papier.

SUEZ biedt ook de mogelijkheid voor de afvoer en vernietiging van digitale datadragers. Meer informatie hierover staat op de site van Campus & Facilitiy Management[3].

## 2.2 HERGEBRUIK

Hergebruik van gegevensdragers is alleen toegestaan als het mogelijk is om de gegevens op de drager volledig te wissen. Anders MAG een gegevensdrager NIET opnieuw worden gebruikt.

Harde schijven (HDD) kunnen veilig worden gewist. LISA adviseert het gebruik van KillDisk[4] van LSoft Technologies Inc.

KillDisk MAG NIET worden gebruikt om gegevens op Solid-State Disks (SSD) te wissen[5].

Wanneer een gegevensdrager wordt gewist, zal KillDisk de gebruiker een certificaat presenteren met de gebruikte wismethode. Het certificaat MOET aan de gegevensdrager worden gehecht. Bij hergebruik van de gegevensdrager KAN de nieuwe gebruiker het certificaat verwijderen.

---

[1] Algemene Verordening Gegevensbeschereming; https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg
[2] Bijvoorbeeld printers en scanners slaan informatie (tijdelijk) op op interne gegvensdragers.
[3] https://www.utwente.nl/en/service-portal/services/cfm/maintenance/sorting-waste-materials
[4] https://www.killdisk.com/eraser.html
[5] Een uitzondering wordt gemaakt wanneer de schijf een SATA-schijf is die rechtstreeks is aangesloten op een computer met het Linux-besturingssysteem. In dit geval kan Secure Erase worden gebruikt om alle gegevens veilig te wissen.

USB-schijven, ofwel thumbdrives of externe SSD's of HDD's, MOGEN NIET opnieuw worden gebruikt en MOETEN in plaats daarvan worden vernietigd.

# 3 SPECIFIEKE RICHTLIJNEN

## 3.1 SERVERS

Servers[6] bevatten meestal een of meer HDD's of SSD's.

Bij het buiten gebruik stellen van een server dienen de gegevensdragers te worden behandeld volgens de basisrichtlijnen (hoofdstuk 2).

Voor servers die door LISA worden onderhouden, is vernietiging van alle gegevensdragers middels een professionele shredder[7] standaard. Dit om te voldoen aan ISO 27001 en NEN 7510 certificeringen.

LISA houdt een logboek bij van alle schijven die op een van beide manieren zijn afgevoerd.

## 3.2 WERKSTATIONS

Een gebruiker kan een verzoek indienen om zijn persoonlijke werkstation te kopen. Indien ze hiervoor toestemming krijgen, MOETEN ze het werkstation aanbieden aan LISA Servicedesk ICT. Meegeleverde gegevensdragers MOETEN worden gereedgemaakt voor hergebruik volgens hoofdstuk 2.2.

## 3.3 (SMART)PHONES

Alleen smartphones met volledige versleuteling van gegevens MOGEN worden hergebruikt. Raadpleeg de handleiding van de fabrikant of de handleiding van het besturingssysteem voor manieren om alle gegevens veilig van de telefoon te wissen.

Alle andere telefoons MOETEN veilig en milieuvriendelijk worden vernietigd.

Telefoons MOGEN NIET worden versnipperd of, op andere manieren, mechanisch vernietigd. De batterij kan brand en explosies veroorzaken.

## 3.4 ANDERE DATADRAGERS

Andere, niet eerder genoemde gegevensdragers, MOETEN veilig en milieuvriendelijk worden vernietigd conform hoofdstuk 2.1.

[6] In het kader van deze richtlijnen worden Network Attached Storage en Storage Area Network-systemen beschouwd als servers.
[7] https://satrindtech.com/