



IT-AA-O-047-0308

Digitaalse info hävitamine

Juhend

Koostas: Valdo Praust

ANNOTATSIOON

Käesolev dokument käsitleb digitaalsete turvalise hävitamise probleematikat ja on määratud praktiliseks juhendmaterjaliks. Töö on koostatud Rahvusarhiivi tellimusel ning on mõeldud eeskätt soovituslike juhiste arhiivimoodustajatele.

Töö algusosas on lühidalt vaadeldud digitaalsete eripära võrreldes traditsiooniliste teabeliikidega ning mitmesuguseid andmekandjate tüüpe, mis nõuavad hävitamisel erinevate meetodite kasutamist. Töö peamine osa on kolme hävitusemeetodi — andmete ülekirjutamise, magnetilise kustutamise ning andmekandja hävitamise — detailne kirjeldus koos viidete ja soovitustega.

Juhendi lissasse on paigutatud andmete magnetilist kustutamist ning andmekandjate hävitamist käsitlevate Euroopa standardite refereeringud, samuti lühiülevaade andmete ja digitaalsete arhivaalide hävitamise eeskirjadest ja headest tavadest.

SISUKORD

Annotatsioon.....	2
1. SISSEJUHATUS.....	5
1.1. Töö eesmärk.....	5
1.2. Taust	5
1.3. Põhimõisted	6
1.4. Konfidentsiaalsusrisk andmete hävitamisel.....	7
1.5. Andmete turvalise hävitamise eesmärk	8
1.6. Kasutatud allikad	9
2. DIGITAALANDMETE TURVALISE HÄVITAMISE ÜLDPÕHIMÕTTED	11
3. ANDMETE KUSTUTAMINE ANDMEKANDJALT	13
3.1. Teisaldatavate andmekandjate ja kohtkindlate andmekandjate erinevused	13
3.2. Andmete turvalise kustutuse põhimõtted.....	14
3.3. Nõuded turvalise kustutuse tarkvarale	14
3.4. Sobivad turvalise kustutuse programmid.....	14
4. SALVESTISE KUSTUTAMINE MAGNET-ANDMEKANDJALT	16
4.1. Meetodid	16
4.2. Magnetsalvestise kustutamise seadmed	16
5. ANDMEKANDJA FÜÜSILINE HÄVITAMINE.....	19
5.1. Füüsilise hävitamise rakendamine	19
5.2. Andmekandjate füüsilise hävitamise seadmed	20
6. JUHISED ANDMETE HÄVITAMISEKS PEAMISTE ANDMEKANDJATÜÜPIDE PUHUL....	22
6.1. Diskett.....	22
6.2. CD.....	23
6.3. DVD	23
6.4. ZIP-ketas	23
6.5. Magnetlindid jms.....	24
6.6. Pooljuhtmälu	24
6.7. Kõvaketas	25
7. KOKKUVÕTE	26

LISA 1. ANDMETE TURVALISE HÄVITAMISE STANDARDID	27
L 1.1. Ülevaade	27
L 1.2. Purustite klassifitseerimise standardid DIN 32757-1 ja DIN 32757-2.....	28
L 1.3. purusti andmik din 32757-2 järgi	31
L.1.3 Magnetsalvestiste kustutuse seadmete klassifitseerimise standard DIN 33858.....	36

1. SISSEJUHATUS

1.1. TÖÖ EESMÄRK

Käesoleva töö eesmärk on luua digitaalandmete hävitamise üldine soovituslik juhendmaterjal. Töö peamiseks adressaadiks on arhiivimoodustajad ning nende (IT-)töötajad, keda see peaks abistama infosüsteemide projekteerimisel ja ehitamisel, hävitamiseks vajalike seadmete ja tarkvara soetamisel ning detailsemate hävituseeskirjade koostamisel konkreetse asutuse tarbeks. Arvestades arhiivinduse spetsiifikat ning selle üsnagi hiljutist põimumist infosüsteemide ja IT maailmaga, on töö algusse lisatud ka lühike sissejuhatav osa.

1.2. TAUST

Kuni viimase ajani sisaldasid arhiivid valdavas enamikus paberdokumente. Arhiveerimise ja arhiivide maailm on infotehnoloogiaga põimunud alles viimastel aastatel.

Digitaalarhivaali mõiste ilmus esmakordselt Vabariigi Valitsuse 29. detsembri 1998. aasta määrusega nr 308 kinnitatud **arhiivieeskirja** (RT I 1998, 118/120, 1904; 2003, 26, 162; 2002, 32, 193; 2002, 32, 193; 2001, 13, 59), mis jõustus 1999. aasta 1. jaanuarist. Selles eeskirjas on muuhulgas sätestatud ka arhivaalide hävitamise üldpõhimõtted, mis on rakendatavad ka digitaalarhivaalidele:

104. Arhivaal hävitatakse:

- 1) arhivaali füüsilise hävitamise teel (purustamine, põletamine jm) või*
- 2) teabe kustutamisega selle kandjalt.*

Arhiivieeskirjas ei ole aga täpsemalt määratletud, kuidas ning millistel tingimustel toimub andmekandja füüsiline hävitamine või teabe kustutamine.

Käesolev töö täidabki selle arhiivieeskirja punkti 104 konkreetse sisuga, andes digitaalarhivaalide hävitamiseks konkreetset ja täpsed juhised, mis tuginevad rahvusvahelistele standarditele ning IT headele tavadele ja reeglitele.

1.3. PÕHIMÕISTED

Informatsioon ehk teave on igasugune teadmus, mis puudutab ükskõik milliseid asju (objekte) — fakte, sündmusi, protsesse, ideid jne — ning millel on teatavas kontekstis teatav eritähendus.

Informatsioon on oma olemuselt abstraktne mõiste, millel iseenesest puudub vorm. Konkreetse kuju võtab ta mingi esitusviisi, sealhulgas andmete ja nende esitusviisi kaudu.

Andmed on informatsiooni taastõlgendatav esitus (nt kirjapanek) mingil eelnevalt kokkulepitud formaliseeritud kujul, mis võimaldab informatsiooni edastada (sh säilitada), tõlgendada ja/või töödelda.

Digitaalandmed on andmed kahendkujul, mille puhul igat liiki teabe — teksti, heli, pildi, video jne — esituseks kasutatakse ainult kahest märgist (0 ja 1) koosnevat tähestikku ning mida rakendatakse tehniliste seadmete abil, mis on võimelised andmeid sellisel kujul salvestama, lugema, edastama ja töötleva. Informatsioon võib olla talletatud paljudel eri viisidel — raiutud kivisse, kirjutatud paberilehele, salvestatud heliplaadina jne. **Kõik arvutiga töödeldavad andmed on alati digitaalandmed.**

Infokandja on töövahend, millesse on talletatud informatsioon nähtaval kujul ja/või tehniliste vahendite abil loetava nähtamatu salvestisena. Peamised infokandjate liigid on paber (näiteks tekstid, joonised, fotod), film ja salvestuskandjad (näiteks magnetlindid, magnetkettad, optilised kettad, pooljuhtsalvestid).

Andmekandja on salvestuskandja, millele salvestatakse digitaalandmeid.

Vorming (*format*) on reeglistik, mis võimaldab digitaalandmeid üheselt interpreteerida. Maailmas on massiliselt kasutusel suur hulk teksti-, heli-, pildi- ja videovorminguid, samuti eriotstarbelisi andmevorminguid, mis võivad olla suhteliselt universaalsed või olla määratud kasutamiseks mingi konkreetse tarkvaratoote, andmebaasisüsteemi, võrguteenuse või muu vahendiga.

Eri vorminguid toetavad tavaliselt arvutis erinevad tarkvaravahendid, mis on võimelised neid vorminguid lugema ning tihti ka muutma ja/või salvestama. Samuti on nad võimelised tegema andmetele vastava informatsiooni inimesele tajutavaks — näitama tekstifailile vastavat teksti arvutiekraanil, kuvama pildifailile vastavat pilti, mängima helifailis salvestatud muusikapala jms.

Kuni 1980.–1990. aastateni oli valdav enamik inimkonna poolt loodud teavet paberdokumentidel ning foto-, filmi- ja helikogudes. Alates 1990ndatest on üha

suuremat kaalu omandamas paberita asjaajamine, mille puhul andmed jäävad digitaalseks kogu oma elutsükli kestel, st neid ei prindita paberile ega teisendata mingisse muusse talletusvormi:

- nad luuakse arvuti abil digitaalselt;
- neid kasutatakse digitaalkujul (neid loetakse arvutiekraanilt või nad juhivad mingite arvutiga ühendatud seadmete tööd);
- neid hoitakse digitaalkujul kas arvuti kõvakettal või vahetatavail andmekandjatel;
- neid töödeldakse (muudetakse) vajadusel arvuti abil digitaalkujul;
- neid edastatakse digitaalkujul, enamasti üldkasutatava andmesidevõrgu (Interneti) kaudu;
- säilitamisvajaduse lõppemisel digitaalandmed hävitatakse kas andmekandja hävitamise või andmete kustutamise teel.

1.4. KONFIDENTSIAALSUSRISK ANDMETE HÄVITAMISEL

Igapäevase bürootöö käigus käepäraste vahenditega sooritatav andmete hävitamine (tekstiosade ja failide kustutus, paberdokumentide purustus lihtsaima paberihundiga jms) kõrvaldab küll tarbetud andmed käibelt, kuid ei kaitse kõrvaldatud andmete konfidentsiaalsust sihiteadlike rünnete eest.

Andmete kustutus operatsioonisüsteemi või rakendustarkvara **kustutuskäskudega** on tegelikult ainult näiline: kõrvaldatakse küll tavalistel töövahenditel põhinev juurdepääs andmetele, andmed ise aga võivad kettal osaliselt või täielikult säilida ning neid on sealt sageli võimalik lugeda isegi mingi teise rakendusprogrammi abil, seda enam aga spetsiaalsete ründeprogrammidega.

Kettal olevaid andmeid ei hävita ka nende **ühekordne ülekirjutus** muude andmetega: tavaline kettaseade tõlgendab küll sellist salvestist ainult pealekirjutatud andmetena, tegelikult aga on iga biti magnetilises esituses väikesed erinevused, mis sõltuvad selle biti alla jäänud biti väärtusest ning laboratoorsete vahenditega on võimalik tuvastada, millist endist väärtust uute andmete biit katab.

Paberdokumentide **purustamine lihtsaima paberihundiga** pikiribadeks andis teatavat kaitset elementaarse visuaalse analüüsi eest. Nüüdseks aga on sooritatud

edukaid ründeid, mis põhinevad ribade skannimisel ja nende automatiseeritud ühendamisel intellektitehniliste ründeprogrammide abil.

Analoogiliste ründemeetodite tõttu on ebatõhus ka magnetkandjate ja laserketaste **jäme tükeldamine**.

Niisiis nõuab hävitatud andmete konfidentsiaalsuse säilitamine igapäevastega võrreldes tõhusamaid meetmeid.

1.5. ANDMETE TURVALISE HÄVITAMISE EESMÄRK

Käesolev juhend käsitleb digitaalandmete turvalist hävitamist mitmesuguste andmekandjate ning andmetalletusviiside korral. Turvalisuse ideaalkriteeriumiks on seejuures tingimus, et hävitatud andmed ei ole pärast hävitamist enam loetavad, st neis sisaldunud informatsioon ei ole enam kättesaadav.

Tegelikkuses on ideaalkriteeriumi taotlemine seotud aja- ja ressursikuluga, seetõttu tuleb taotleda põhjendatud tasakaalu konfidentsiaalsuse rikkumisest tuleneva kahju ja turvakulude vahel. Hävitatud andmete täieliku käideldamatuse taotlemise asemel **tuleb tagada andmete kaitse sellisel määral, et rünnakuks kulutatav aeg ja ressursid kaaluvad üle saadava info konfidentsiaalsusväärtuse**.

Konfidentsiaalsusnõuete ja -tasemete eristamisel on käesolevas töös aluseks võetud 1998. aastal Cybernetica ASi poolt Eesti Informaatikakeskuse tellimisel koostatud töö "Turvaklasside kirjeldused" ([1], DO-ST-X-09-0803), mis on viimastel aastatel leidnud nii avaliku sektori kui osalt ka erasektori andmete turvaalasel liigitamisel laialdast kasutust.

Nimetatud töö jagab andmed nende konfidentsiaalsusnõuete järgi nelja alljärgnevasse klassi:

- **Klass S0. Avalik teave, mida võivad kasutada kõik soovijad.**
- **Klass S1. Teave, mille avalikustamine võib põhjustada materiaalsel või moraalsel kahju.** Sellesse klassi võib paigutada näiteks asutuse või ettevõtte töötajate palgaandmed, mille avalikustamine konkurentidele ja ka teistele töötajatele võib põhjustada asutusele materiaalsel kahju, samuti asutuse sisemist töökorraldust puudutavad andmed.
- **Klass S2. Teave, mille avalikustamine häirib riigi või asutuse talitlust või rikub inimese privaatsust.** Riigile tähendaks selliste andmete avalikustamine

miljonitesse ulatuvaid kahjusid, ettevõttele aga kahjusid, mis ulatuvad kümne protsendini aastakäibest.

Sellesse klassi võib paigutada näiteks teabe, mille leke võib häirida riigikaitset või diplomaatiat, põhjustada välis- ja sisepoliitilisi kriise, nõrgestada majandust. Kõik delikaatsed isikuandmed võiksid olla konfidentsiaalsusega S2, samuti ka need isikuandmed, mille avalikustamine on ära keelanud isik ise. Sellesse klassi kuuluvad ka poliitikat ja majandust laias ulatuses puudutavate õigusaktide vahevariandid ja mustandid, mis võivad põhjustada segadusi enne ametliku lõppvariandi valmimist. Eraettevõtte võib liigitada klassi S2 näiteks kogu tulevaste äriideedega seotud teabe, mille avalikustamine oleks kasulik konkurentidele ja võiks tunduvalt vähendada ettevõtte tulusid. Riikliku registri pidajad võivad sellesse klassi liigitada kõik paroolid, mille abil on võimalik saada piiratud lugemis- ja modifitseerimisõigusi registri andmete kasutamiseks.

- **Klass S3. Teave, mille avalikustamine on ohtlik riigi, asutuse või inimese turvalisusele või on vastuolus inimõigustega, samuti teave, mille avalikustamine võib põhjustada kontrollimatuid muudatusi riigile või asutusele tähtsates infosüsteemides.** Riigile tähendaks selliste andmete avalikustamine eelarvega võrreldavaid kahjusid, ettevõttele tema aastakäibega võrreldavaid kahjusid.

Sellesse klassi võib paigutada näiteks teabe uute relvade hankimise ja väljatöötamise kohta, kui selle leke võiks ohustada nende relvade riigikaitse eesmärgil kasutamise tõhusust ja seeläbi nõrgendada riigi kaitsevõimet. Iga ettevõtte võib liigitada klassi S3 kõik sellised andmed, mille avalikustamine seab ohtu ettevõtte eksistentsi. Sellesse klassi võivad kuuluda ka näiteks kohtuprotsessidesse kaasatud oluliste tunnistajate isikuandmed, mille avalikustamine seaks ohtu tunnistajate elu. Kõiki pääsuandmed, mis võimaldavad piiramatu tegutsemist riiklikult tähtsates andmekogudes (näiteks põhiregistris) ja põhjustada sellega kaost riigis, võib samuti lugeda klassi S3 kuuluvateks. Iga ettevõtte võib liigitada klassi S3 andmeteks näiteks oma süsteemiülemate paroolid ja kasutatavad krüpteerimisvõtmed, sest nende avalikustamine võib põhjustada andmekogude hävingut ja delikaatsete isikuandmete ulatuslikku leket.

1.6. KASUTATUD ALLIKAD

1. Turvaklasside kirjeldused. Tehniline aruanne DO-ST-X-09-0803. Küberneetika AS, 1999.
2. DIN 32757-1. Büro- und Datentechnik — Vernichten von Informationsträgern — Teil 1: Anforderungen und Prüfungen an Maschinen und Einrichtungen.

3. DIN 32757-2. Büro- und Datentechnik; Vernichten von Informationsträgern — Teil 2: Maschinen und Einrichtungen; Mindestangaben.
4. DIN 33858. Büro- und Datentechnik; Löschen von schutzbedürftigen Daten auf magnetischen Datenträgern; Löscheräte, Anforderungen und Prüfungen.
5. IT-Grundschutzhandbuch / IT Baseline Protection Manual. Deutsches Bundesamt für Sicherheit in der Informationstechnik (BSI), <http://www.bsi.de/>, 1996-2003.

2. DIGITAALANDMETE TURVALISE HÄVITAMISE ÜLDPÕHIMÕTTED

Digitaalandmeid on andmekandjatele võimalik salvestada kahel erineval põhimõttel:

1. **Andmed salvestatakse andmekandjale püsivalt**, nii et salvestist ei saa andmekandjalt enam põhimõtteliselt eemaldada ega ümber kirjutada. Seda moodust kasutatakse praegu peamiselt CDde ja DVDde puhul. Neile on võimalik andmeid salvestada nii andmekandjate tööstusliku masstiražeerimisena kui ka kasutaja arvutis oleva kirjutusseadmega. Enamasti kasutatakse püsisalvestamist teistsaldatavate andmekandjate puhul.
2. **Andmed salvestatakse korduvkirjutavale andmekandjale**. Levinuim korduvkirjutav andmekandja on praegu arvutis sisalduv kõvaketas, mis võimaldab sinna salvestatud andmete paljukordset ümberkirjutamist. Korduvkirjutust võimaldab ka hulk teistsaldatavaid andmekandjaid — CD-RWd, disketid, magnetlindid (sh DAT-lindid), väikmäälud (*flash memory*) jt.

Digitaalandmete turvalise hävitamise seisukohalt tuleb eelnimetatud kahte tüüpi andmekandjatega toimida erinevalt:

- **Korduvkirjutavale andmekandjale salvestatud andmeid võib hävitada andmete kustutamise — täpsemalt öeldes uute andmetega ülekirjutamise — teel.**
- **Andmekandjale püsivalt salvestatud andmeid saab hävitada ainult andmekandja füüsilise hävitamise teel.** Füüsilise hävitamise meetod peab tagama, et andmekandjalt või selle jäänustelt/tükkidelt ei oleks sinna salvestatud andmed enam loetavad.
- **Korduvkirjutatavatelt defektsetelt andmekandjatel saab andmeid turvaliselt hävitada samuti ainult andmekandja füüsilise hävitamise teel.** See välistab nt võimaluse, et konfidentsiaalseid andmeid sisaldava rikkiläinud ning ära visatud kõvaketta suudab selle leidja siiski korda teha ning sellele salvestatud andmeid välja lugeda.

Seega peab digitaalandmete turvaline hävitamine hõlmama nii andmekandjate hävitamist kui ka neile salvestatud andmete turvalist kustutamist.

Avalikku (konfidentsiaalsusklassiga S0) teavet sisaldavate andmekandjate või andmete hävitamisel ei ole vaja spetsiaalseid turvanõudeid rakendada:

- 1. Avalike andmete kustutamisel korduvkirjutatavatelt andmekandjatelt võib kasutada operatsioonisüsteemi või rakendustarkvara enda vahendeid, hoolimata asjaolust, et andmed on kustutamise järgselt süsteemsete vahenditega taastavad.**
- 2. Andmekandjale püsivalt salvestatud avalike andmete hävitamiseks võib andmekandja lihtsalt ära visata.** Seejuures peab järgima kehtiva jäätmeseaduse ning selle rakendusaktide nõudeid, samuti andmekandja valmistaja soovitusi andmekandja utiliseerimiseks. Näiteks ei tohi enamikke andmekandjaid põletada tulekolletes, kuna nende valmistamiseks kasutatav plast võib põlemisel tekitada mürgiseid gaase.
- 3. Andmete hävitamiseks korduvkirjutatavatelt, aga defektsetelt andmekandjatelt võib samuti andmekandja lihtsalt ära visata,** kui rakendatakse jäätmeseaduse ja selle rakendusaktide nõudeid.

Punktide 2 ja 3 juures tuleb arvestada, et nii võib käituda andmekandjatega, mis sisaldavad **ainult** avalikke (konfidentsiaalsusklassiga S0) andmeid. **Kui kasvõi osal andmetest on klassist S0 kõrgem konfidentsiaalsustase, tuleb rakendada peatükkides 3–6 kirjeldatud nõudeid.**

3. ANDMETE KUSTUTAMINE ANDMEKANDJALT

Andmeid saab kustutamisega hävitada korduvkirjutatavatel teisaldatavatel andmekandjatel, kui andmete lugemisel ja/või kirjutamisel ei ole esinenud tehnilisi probleeme.

3.1. TEISALDATAVATE ANDMEKANDJATE JA KOHTKINDLATE ANDMEKANDJATE ERINEVUSED

Kohtkindlad ehk statsionaarsed andmekandjad, nt arvuti kõvaketas, on tavaliselt seade, millesse on sisse ehitatud teatud juhtplokid, mis on vajalikud andmekandjalt lugemiseks ja sinna kirjutamiseks, samuti vahetult ketta poole pöörduv lugemis- ja kirjutamispea. Kogu andmekandja koos juhtplokkide ning lugemis-kirjutamispeaga paikneb ühtses ning sageli avamatus korpuses. Seetõttu ei pruugi kõvaketta tõrge tähendada alati sinna salvestatud salvestise kustumist või kahjustumist kettapinnal, selle põhjuseks võib olla juhtplokkide või lugemis-kirjutamispea rike.

Seetõttu tuleb kohtkindel ehk statsionaarne andmekandja rikke korral kas füüsiliselt hävitada (vt ptk 5) või spetsiaalse kustutusseadmega ümber magneetida (vt ptk 6).

Teisaldatavad korduvkirjutatavad andmekandjad (CDd, DVDd, magnetlindid jne) tavaliselt ei sisalda juhtplokkide ega lugemis-kirjutuspäid, vaid ainult kandjat (plaati, linti vm) ennast. Kui selline andmekandja läheb rikki, tuleb ta füüsiliselt hävitada (vt ptk 5) või magnetilise salvestusmeetodi abil ümber magneetida (vt ptk 6). Põhimõtteliselt võib ümber magneetida ka tehniliselt korras korduvkirjutatavaid andmekandjaid (nt DAT-linti, ZIP-ketast vms), kui neil asuvaid andmeid soovitakse hävitada ning andmekandjaid endid ei soovita enam säilitada.

Üldiselt saab korduvkirjutatavalt andmekandjalt andmeid hävitada nende kustutamise teel.

3.2. ANDMETE TURVALISE KUSTUTUSE PÕHIMÕTTED

Andmete turvaliseks kustutamiseks andmekandjalt ei sobi tavalised operatsioonisüsteemi kustutuskäskud — *delete*, *erase* vms. Põhjus on selles, et need jäätavad tegelikult failile vastava informatsiooni — bitijärjestused — kettale füüsiliselt alles, kustutades vaid kettakasutustabelist lahtrid, mis viitavad faili füüsilisele asukohale kettal. Seetõttu saab näiteks ka ekslikult kustutatud faili hiljem taastada.

Faili turvaliseks kustutuseks korduvkirjutatavalt andmekandjalt tuleb see kirjutada üle ühtlase tõenäosusjaotusega juhusliku bitijadaga. Turvalisuse kaalutlustel tehakse seda tavaliselt mitu korda järjest, tüüpiline on kustutatavate andmete kolmekordne ülekirjutus. Selleks kasutatakse spetsiaalset kustutustarkvara.

3.3. NÕUDED TURVALISE KUSTUTUSE TARKVARALE

Andmete andmekandjalt turvaliseks kustutamiseks kasutatav algoritm peab vastama alljärgnevale tingimustele:

- 1) **kustutatavad andmed tuleb selle bitijadaga üle kirjutada konfidentsiaalsustaseme S1 korral vähemalt korra, konfidentsiaalsustasemete S2 ja S3 korral aga vähemalt kolm korda järjest.**
- 2) **kasutataval juhuslikul bitijadal peab olema matemaatilises mõttes valge müra omadustega, st genereeritav bitijada ei tohi statistiliste ega muude meetoditega olla eristatav tõelisest ühtlase tõenäosusjaotusega juhujadast (nn valgest mürast).**

Olemasolevaid turvalise kustutamise programme tuleb enne kasutuselevõtmist nende kolme omaduse osas testida või veenduda, et see test on juba varem sooritatud. Kui kirjutada turvalise kustutuse programm ise, tuleb need kolm tingimust võtta programmeerimisülesande lähtetingimusteks.

3.4. SOBIVAD TURVALISE KUSTUTUSE PROGRAMMID

Jaotises 3.3. esitatud turvalise kustutuse programmi tingimustele vastavad näiteks alljärgnevad levinud tarkvaratooted:

- **PGP**; levitatakse priivarana; sobivad kõik versioonid; saadaval on ka lähtetekstid; <http://www.pgp.com/>

- **Secure Wipe**, kõik versioonid, <http://www.alpinesnow.com/sw.shtml>
- **BCWipe**, <http://www.jetico.com/>
- **CyberScrub**, <http://165.121.190.90/home.html>
- **DECLASFY**, <http://www.dmares.com/maresware/df.htm#DECLASFY>
- **DiskZapper**, <http://diskzapper.com/>
- **East-Tec File Shredder v1.0**, <http://www.east-tec.com/erprod/etfshred/index.htm>
- **Eraser**, <http://www.heidi.ie/eraser/>
- **Fwipe**, <http://www.nb.net/~lbudney/linux/software/fwipe.html>
- **Grind**, <http://www.m-rosenkranz.de/grind/index.php>
- **KillFile**, <http://www.wilter.com/epicurus/>
- **NTWipe**, <http://www.dmares.com/maresware/lo.htm#NTWIPE>
- **SecureClean**, <http://www.AccessData.com>
- **Shred-X**, <http://www.bsoft.ic24.net/>
- **Without A Trace**, <http://online.securityfocus.com/tools/1027>

Sobivaid turvalise kustutuse programme on muidki, kuid loetletud on levinumaid, millele viitavad maailma mitmed andmeturbeallikad. Nimetatuist erineva tarkvara kasutamise soovi korral tuleb teda testida jaotises 3.3. esitatud kolme kriteeriumi suhtes.

4. SALVESTISE KUSTUTAMINE MAGNET-ANDMEKANDJALT

4.1. MEETODID

Magnetilise salvestusviisiga andmekandjalt on võimalik lisaks failide turvalise kustutamise moodustele (vt jaotised 3.3. ja 3.4.) andmeid kustutada ka spetsiaalsete seadmetega (*degausser*), mis kasutavad selleks ülitugevat magnetvälja. Sellise magnetvälja rakendamise tulemuseks on andmekandja magnetkihi ümbermagneetimine (otstarbe seisukohalt: demagneetimine).

Kui magnetilise salvestusviisiga andmekandja kasutamisel on esinenud tõrkeid, (nt defektseid sektoreid) tuleb andmete hävitamisel igal juhul kasutada kas käesolevas jaotises käsitletavat kustutust magnetväljaga või peatükis 5 vaadeldud mehaanilist hävitamist. Sellistelt andmekandjalt ei tohi andmeid kustutada peatükis 3 vaadeldud mitmekordse ülekirjutuse meetodiga, sest osa loetamatuks muutunud piirkondi võib sel juhul kettal säilida ning olla edaspidi loetavad.

4.2. MAGNETSALVESTISE KUSTUTAMISE SEADMED

Magnetilise salvestise kustutamise seadmetel (*degausser*) on kaks olulist tehnilist näitajat:

- **kustutustugevus** (*depth of erasure*), mida mõõdetakse detsibellides;
- **kustutatava andmekandja maksimaalne koertsitiivväljatugevus** (*coercivity figure*), mida seade on võimeline kustutama nii, et andmed ei oleks andmekandjalt enam loetavad.

Koertsitiivväljatugevus sõltub andmekandja salvestustihedusest. Tüüpilistel andmekandjatel on ta alljärgnev:

Tüüpilised magnetkandjate koertsitiivväljatugevused, örstedites (Oe)	
5,25" 360 KB diskett	300
5,25" 1,2 MB diskett	675
3,5" 720 KB diskett	300
3,5" 1,4 MB diskett	700
1980. aastate kõvakettad	1400
1990. ja 2000. aastate kõvakettad	2200
1/2" magnetlint	300
1/4" QIC-lint	550
8 mm, metalliosakestega lint	1500
DAT-lint	1500

Väljatugevus 1 Oe = $1000/4\pi$ A/m.

Eesti tingimustes võib kasutada sellist magnetsalvestise kustutuse seadet, kui

- **kustutustugevus on konfidentsiaalsusklassi S1 korral vähemalt 45 dB, konfidentsiaalsusklasside S2 või S3 korral aga vähemalt 90 dB;**
- **seadet kasutatakse selliste andmekandjate kustutamiseks, mille koertsitiivväljatugevus ei ole suurem kui seadme tehnilises kirjelduses esitatud väärtus.**

Tavaliselt on magnetsalvestise kustutuse seadme tootetutvustuses esitatud loetelu andmekandjatest, mida ta on võimeline jäädavalt kustutama, ning ka seadme kustutustugevus.

Lähtudes standardis DIN 33858 toodud magnetsalvestise kustutusseadmete klassifikatsioonist ning tähistest (vt standardi refereering jaotises L 1.4), tuleb seadme soetamisel ja kasutamisel juhinduda järgnevatest reeglitest:

- **konfidentsiaalsustasemega S1 andmete kustutamisel peab kustutusseade vastama DIN 33858 A-taseme nõuetele;**
- **konfidentsiaalsustasemega S2 või S3 andmete kustutamisel peab kustutusseade vastama DIN 33858 B-taseme nõuetele;**
- **DIN 33858 klassidele A1 ja B1 vastavad seadmed ei kõlba oma madala koertsitiivväljatugevuse tõttu praktiliselt enam ühegi kaasaegse andmekandja turvaliseks kustutamiseks** (viietolline diskett on infotehnika ajalugu; vrd eeltoodud tabel ning jaotises L 1.4. esitatud tasemete kirjeldused);
- **DIN 33858 klasside A2 ja B2 seadmed kõlbavad praktiliselt vaid diskettide ning vanema tehnoloogiaga magnetlintide turvaliseks kustutamiseks; DAT- lintide, kõvaketaste jpt andmekandjate kustutamiseks nad ei sobi;**
- **kõvaketaste ning kõikide teiste kaasaegsete digitaalsete magnetsalvestiste turvaliseks kustutamiseks kasutatav seade peab vastama DIN 33858 klassi A3 või B3 nõuetele.**

Seega on arhiivi, andmepanga vms tarbeks otstarbekas hankida seade, mille koertsitiivväljatugevus on vähemalt võrdne seal kasutatava maksimaalse tihedusega andmekandja omaga. Kui hoitavate andmete hulgas on kasvõi vähesel määral andmeid konfidentsiaalsustasemega S2, tuleb igal juhul soetada B-klassi seade.

Peale selle tuleb pidada silmas, et **magnetilise salvestise kustutamise seadmete (*degausser*) kasutamine on praktiliselt ainus moodus, millega saab defektsetelt kõvaketastelt konfidentsiaalse teabe turvaliselt kustutada**. Seetõttu on kõvaketaste turvalise kustutamise vajaduse korral mõistlik soetada turvaklassile A3 või B3 vastav kustutusseade.

5. ANDMEKANDJA FÜÜSILINE HÄVITAMINE

5.1. FÜÜSILISE HÄVITAMISE RAKENDAMINE

Andmekandjate füüsiline hävitamine on kindlaim viis neile salvestatud andmete jäädava loetamatuse tagamiseks.

Andmekandjate füüsilist hävitamist rakendatakse nelja tüüpi andmekandjate puhul; kahel juhul on füüsilisele hävitamisele alternatiiv, kahel mitte.

1. **Püsisalvestusega andmekandjate** korral on andmekandja füüsiline hävitamine ainus viis andmete jäädavaks hävitamiseks.
2. **Tehniliselt korras korduvkirjutavat andmekandjat** võib andmete kustutamiseks küll füüsiliselt hävitada, kuid sellega samaväärne andmete hävitusviis on andmete turvaline kustutamine (vt jaotised 3.2–3.4).
3. **Täielikult või osaliselt defektset** (osa salvestusruumi ei ole kasutatav, kõvakettal nt defektsed sektorid (*bad sectors*)) **korduvkirjutavat magnetilist andmekandjat** võib hävitada füüsiliselt või kustutada magnetiliselt jaotises 4.2 mainitud tingimustele vastava seadmega.
4. **Täielikult või osaliselt defektsele** (osa salvestusruumi ei ole kasutatav, kõvakettal nt defektsed sektorid) **korduvkirjutavale mittemagnetpõhisele andmekandjale** — nt korduvkirjutavale CDle, nn CD-RWle — salvestatud andmete hävitamise ainus viis on andmekandja füüsiline hävitamine.

Andmekandjad hävitatakse füüsiliselt **enamasti nende mehaanilise purustamise teel**. Põhimõtteliselt saab neid hävitada ka termiliselt (nt põletamise teel), keemiliselt vm viisil, kuid need võtted ei ole eriti levinud, samuti on need tihti vastuolus keskkonnakaitse eeskirjadega.

5.2. ANDMEKANDJATE FÜÜSILISE HÄVITAMISE SEADMED

Andmekandjate füüsilise hävitamise seadmed on tavaliselt võimsamat laadi paberihundid (*shredder*), mis on võimelised purustama üsna paksudele paberipakkidele lisaks ka diskette, CDsid, DVDsid, ZIP-kettaid jm teisaldatavaid andmekandjaid. Nii nagu pabermaterjalid purustatakse ka andmekandjad peenteks tükkideks. Nende seadmete kõige olulisemad näitajad on töökiirus, purustatava materjali paksus (või andmekandja tüüp) ja purustusaste (osakeste suurus). Euroopa turul müüdavate purustite korral on viimane tavaliselt esitatud viitena ühele standardis DIN 32757 (vt standardi refereering jaotistes L 1.2 ja L 1.3) spetsifitseeritud tasemeist (1 kuni 5), millele seade vastab.

Sobiva tehnilise lahenduseta on tänini maailmas jäänud kõvaketaste purustamine. Kõvaketaste puhul tuleks võimaluse korral eelistada magnetilist kustutust (vt ptk 4) või meetodeid, mida on kirjeldatud jaotises 6.7.

Eestis tuleb andmekandjate turvaliseks purustamiseks:

- **konfidentsiaalsustaseme S1 korral kasutada purustit, mis vastab DIN 32757 3. tasemele;**
- **konfidentsiaalsustaseme S2 korral kasutada purustit, mis vastab DIN 32757 4. tasemele;**
- **konfidentsiaalsustaseme S3 korral kasutada purustit, mis vastab DIN 32757 5. tasemele.**

NB! Purusti soetamisel tuleb standardile DIN 32757 vastava taseme kindlaksmääramisel olla ülimalt ettevaatlik, sest tasemed 3–5 määratakse paberdokumentide ning suure infoesitustihedusega materjalide (sh andmekandjate) korral tunduvalt erinevalt. Näiteks nõuab standardi 4. tase paberi purustamist mitte suuremateks kui 30 mm² tükkideks, andmekandjate purustamisel nõuab sama tase aga maksimaalselt kuni 0,5 mm² suurusi tükke, seega joonmõõtmetelt peaaegu kuus korda väiksemaid. 5. tase nõuab andmekandjate purustamist maksimaalselt 0,2 mm² suurusteks osakeseks, samal ajal kui 5. tasemele vastav paberdokumentide purustilt nõutakse "kõigest" 10 mm² suurusi tükke.

Kuna mitmed turulolevad purustid peenestavad samade tööorganitega nii paberit kui ka andmekandjaid, on tavaline olukord, kus purusti on paberdokumentide hävitamisel saanud palju kõrgema turvatase kui andmekandjate purustamisel. Kui purustile on antud standardile DIN 32757 vastav(ad) turvatase(med), on seadme kohta täidetud põhjalik ankeet, mis peab sisalduma purusti dokumentatsioonis. Nimetatud ankeet

sisaldub standardis DIN 32757-2 ning selle eestikeelne tõlge on esitatud käesoleva dokumendi lisa jaotises L 1.3. **Mõistlik on enne purusti soetamist uurida põhjalikult tehnilist dokumentatsiooni ning selgitada välja, milliste materjalide purustamisel on sellele turvatasemeid antud.**

6. JUHISED ANDMETE HÄVITAMISEKS PEAMISTE ANDMEKANDJATÜÜPIDE PUHUL

Järgnevalt on konseptiivselt loetletud võtted ja neile esitatavad nõuded andmete hävitamiseks seitsmelt levinumalt andmekandjatüübilt.

6.1. DISKETT

Tehniliselt korras diskett (ilma defektsete sektoriteta):

- **turvaline kustutus**, klassi S1 andmete korral sooritatakse ühekordse ülekirjutusega, klassi S2 või S3 andmete korral vähemalt kolmekordse ülekirjutusega (vt jaotised 3.3–3.4);
- defektselt kettalt andmete hävitamise võtted.

Defektne diskett (sisaldab defektseid sektoreid):

- **magnetiline kustutus** (vt jaotis 4.2) – klassi S1 andmete korral DIN 33858 A2 nõuetele vastava seadmega, klassi S2 või S3 andmete korral DIN 33858 B2 nõuetele vastava seadmega; silmas tuleb pidada, et sageli saab disketti hiljem uuesti vormindada ja kasutusele võtta (vt jaotised 4.2 ja L 1.4);
- **purustamine** – klassi S1 andmete korral vastavalt DIN 32757 3. taseme nõuetele, klassi S2 andmete korral vastavalt DIN 32757 4. taseme nõuetele ning klassi S3 andmete korral vastavalt DIN 32757 5. taseme nõuetele (vt jaotised 3.3–3.4 ja jaotis L 1.2);
- **põletamine lõkkes, ahjus, katlas vm** (NB! Saastab keskkonda!).

6.2. CD

- **purustamine** – klassi S1 andmete korral DIN 32757 3. taseme nõuetele vastavalt, klassi S2 andmete korral DIN 32757 4. taseme nõuetele vastavalt ning klassi S3 andmete korral DIN 32757 5. taseme nõuetele vastavalt (vt 3.3–3.4 ja L 1.2);
- **põletamine lõkkes, ahjus, katlas vm** (NB! Saastab keskkonda!).

6.3. DVD

- **purustamine** – klassi S1 andmete korral vastavalt DIN 32757 3. taseme nõuetele, klassi S2 andmete korral vastavalt DIN 32757 4. taseme nõuetele ning klassi S3 andmete korral vastavalt DIN 32757 5. taseme nõuetele (vt jaotised 3.3–3.4 ja jaotis L 1.2);
- **põletamine lõkkes, ahjus, katlas vm** (NB! Saastab keskkonda!).

6.4. ZIP-KETAS

Tehniliselt korras ketas (ilma defektsete sektoriteta):

- **turvaline kustutus** – klassi S1 andmete korral ühekordse ülekirjutusega, klassi S2 või S3 andmete korral vähemalt kolmekordse ülekirjutusega (vt 3.3–3.4);
- defektselt kettalt andmete hävitamise võtted.

Defektne ketas (sisaldab defektseid sektoreid):

- **magnetiline kustutus** (vt jaotis 4.2) – klassi S1 andmete korral DIN 33858 A2 nõuetele vastava seadmega, klassi S2 või S3 andmete korral DIN 33858 B2 nõuetele vastava seadmega; silmas tuleb pidada, et sageli saab ketast hiljem uuesti vormindada ja kasutusele võtta (vt jaotised 4.2 ning L 1.4);
- **purustamine** – klassi S1 andmete korral vastavalt DIN 32757 3. taseme nõuetele, klassi S2 andmete korral vastavalt DIN 32757 4. taseme nõuetele ning klassi S3 andmete korral vastavalt DIN 32757 5. taseme nõuetele (vt jaotised 3.3–3.4 ja jaotis L 1.2);
- **põletamine lõkkes, ahjus, katlas vm** (NB! Saastab keskkonda!).

6.5. MAGNETLINDID JMS

Tehniliselt korras lint:

- **turvaline kustutus** – klassi S1 andmete korral sooritatakse ühekordse ülekirjutusega, klassi S2 või S3 andmete korral vähemalt kolmekordse ülekirjutusega (vt jaotised 3.3–3.4);
- defektselt lindilt andmete hävitamise võtted.

Defektne lint:

- **magnetiline kustutus** (vt jaotis 4.2) – klassi S1 andmete korral DIN 33858 A3 nõuetele vastava seadmega, klassi S2 või S3 andmete korral DIN 33858 B3 nõuetele vastava seadmega; mõnikord saab hiljem linti uuesti vormindada ja kasutusele võtta, mõnikord aga mitte (vt jaotised 4.2 ja L 1.4);
- **purustamine** – klassi S1 andmete korral vastavalt DIN 32757 3. taseme nõuetele, klassi S2 andmete korral vastavalt DIN 32757 4. taseme nõuetele ning klassi S3 andmete korral vastavalt DIN 32757 5. taseme nõuetele (vt jaotised 3.3–3.4 ja L 1.2);
- **põletamine lõkkes, ahjus, katlas vm** (NB! Saastab keskkonda!).

6.6. POOLJUHTMÄLU

Tehniliselt korras seade:

- **turvaline kustutus** – klassi S1 andmete korral sooritatakse ühekordse ülekirjutusega, klassi S2 või S3 andmete korral vähemalt kolmekordse ülekirjutusega (vt 3.3–3.4);
- defektselt seadmelt andmete hävitamise võtted.

Defektne seade:

- **mehaaniline purustamine** – oma paksuse tõttu on tihti problemaatiline seadme asetamine purustisse, üldiselt peab purusti vastama DIN 32757 5. taseme nõuetele (vt jaotised 3.3–3.4 ja L 1.2);
- **põletamine lõkkes, ahjus, katlas vm** (NB! Saastab keskkonda!).

Kuna levinuimad pooljuhtmälud, välmälud (*flash*) on kasutusel olnud üsna lühikest aega, ei ole veel selle seadme üldtunnustatud turvalisi hävitusmeetodeid välja kujunenud. **Soovitav on selline seade võimalusel põletada**, väikese massi tõttu ei saasta ta oluliselt keskkonda.

6.7. KÕVAKETAS

Tehniliselt korras ketas (ilma defektsete sektoriteta):

- **turvaline kustutus** – klassi S1 andmete korral ühekordse ülekirjutusega, klassi S2 või S3 andmete korral vähemalt kolmekordse ülekirjutusega (vt jaotised 3.3–3.4);
- defektselt kettalt andmete hävitamise võtted.

Defektne ketas (sisaldab defektseid sektoreid):

- **magnetiline kustutus** (vt jaotis 4.2) – klassi S1 andmete korral DIN 33858 A3 nõuetele vastava seadmega, S2 või S3 andmete korral aga DIN 33858 B3 nõuetele vastava seadmega; tuleb silmas pidada, et magnetiliselt kustutatud kõvaketas jääb püsivalt kasutuskõlbmatuks, sest kustutatakse ka tehases kettale kantud vormindusandmed (vt jaotised 4.2 ja L 1.4);
- **põletamine ahjus, katlas vm** (NB! Saastab keskkonda!).

Kõvaketaste purustamiseks puuduvad seni maailmas kehtivad üldised standardid ja juhised (vt nt [5], S 2.167: *Secure deletion of data media*), seetõttu tuleb rikkis kõvakettale jäänud konfidentsiaalsed andmed kustutada eelistatavalt magnetilise kustutamise teel. Alternatiivvariandina on võimalik ka kettaploki lammutamine ning selles asuvate ketaste mehaaniline purustamine. Sel juhul peab see toimuma klassi S1 andmete korral vastavalt DIN 32757 3. taseme nõuetele, klassi S2 andmete korral vastavalt DIN 32757 4. taseme nõuetele ning klassi S3 andmete korral vastavalt DIN 32757 5. taseme nõuetele (vt jaotised 3.3–3.4 ja L.1.2)

Üheks võimaluseks on ka kettaploki termiline hävitamine ahjus, katlas vm, kuid kõvaketas oma küllalt suure massiga (nt välmäluga võrreldes) saastab olulisel määral keskkonda. **Purustamine või põletamine on aga ainuvõimalikud sellise asutuse või firma jaoks, kes ei saa mingil põhjusel endale kallist magnetilise kustutamise seadet soetada.**

7. KOKKUVÕTE

Käesolev juhend annab arhiividele jpt andmevaldajatele konkreetsed juhised, kuidas tuleb hävitada konfidentsiaalseid andmeid levinumatelt andmekandjatelt, ja ülevaate, kuidas andmete hävitamist reguleerivad Euroopa standardid. See on esimene põhjalikum eestikeelne käsitus sellest valdkonnast. Juhend hõlmab andmete turvalise hävitamise kõiki kolme liiki — turvalist ülekirjutamisega kustutamist, andmekandjate füüsilist hävitamist ning välise magnetväljaga magnetilist kustutamist. Loodetavasti paneb juhend aluse heale tavale selles valdkonnas.

Kui andmed on avalikud, st nende konfidentsiaalsustase [1] on S0, võib neid kustutada operatsioonisüsteemi vahenditega ning defektsed andmekandjad võib lihtsalt ära visata. Tuleb aga silmas pidada, et kui ühel defektsel andmekandjal on erineva konfidentsiaalsustasemega andmeid, tuleb andmekandjat käsitseda rangeima konfidentsiaalsusklassi nõuete järgi. Näiteks kui avalikke andmeid sisaldaval CDI on üksikuid S2-klassi andmeid, tuleb CD hävitada tasemele S2 vastavate nõuete kohaselt.

LISA 1. ANDMETE TURVALISE HÄVITAMISE STANDARDID

L 1.1. ÜLEVAADE

Euroopas on üldiselt standarditud kaht meetodit — magnetsalvestiste kustutust salvestivälise magnetväljaga ning andmekandjate füüsilist hävitamist. Muid meetodeid — turvalist kustutust (ülekirjutamist) krüptotehniliste võtetega (vt ptk 3), andmekandjate keemilist ja/või termilist hävitamist, kõvaketaste füüsilist hävitamist jms — mingid tunnustatud standardid ei reguleeri. Nii magnetsalvestiste kustutamisel kui ka andmekandjate purustamisel on faktilisteks Euroopa standarditeks kujunenud Saksa standardid (DIN).

Andmekandjate turvalist purustamist käsitleb standard DIN 32757. See standard koosneb kahest osast:

- DIN 32757-1. „Büro- und Datentechnik — Vernichten von Informationsträgern — Teil 1: Anforderungen und Prüfungen an Maschinen und Einrichtungen“ (Büro- ja arvutitehnika. Infokandjate hävitamine. Osa 1: Nõuded ja teimid* masinatele ja seadmetele);
- DIN 32757-2. „Büro- und Datentechnik; Vernichten von Informationsträgern; Maschinen und Einrichtungen; Mindestangaben“ (Büro- ja arvutitehnika. Infokandjate hävitamine. Masinad ja seadmed. Minimaalnäitajad).

Standardi esimene osa pärineb 1995. aasta jaanuarist ja teine osa 1985. aasta oktoobrist. Suurelt osalt on see standard suunatud paberdokumentide hävitamisele ning vaid vähesel määral ning pealiskaudselt on käsitletud muid infokandjaid — fotosid, mikrofilme, sh ka andmekandjaid. Arvestades viimase kümnendi jooksul toimunud suurt arengut andmekandjate ja andmete tiheduse alal, võib neid standardeid lugeda üsna vananenuteks. Uuemad standardid aga kahjuks puuduvad.

* Teim – laboratoorne katse, teimimine – katseliselt omaduste määramine laboratoorses tingimustes (<http://www.eki.ee/keeleabi/artiklid2/test.html>).

DIN 32757 turvaliigituse, olulisemate nõuete ja tehniliste detailide refereering on esitatud jaotises L 1.2.

Kuna DIN 32757 sätestab mitu purustusklassi ning nendele klassidele vastavad purustatud infokandjate maksimaalmõõtmed (vt jaotis L 1.2), on see standard siiski kasutuskõlblik ka tänapäeval. Tükkide suuruse puhul tuleb aga igal juhul arvestada praegusi (arvutus)tehnilisi võimalusi, mis võimaldavad ribadeks lõigatud andmekandja (disketi, CD vms) kõik ribad automaatselt sisse skannida ning määrata nende algse järjestuse mitte käsitsi, vaid automaatselt, nii et küllalt suurte osade (ribade) korral on veel võimalik teave taastada.

Valdav enamik Euroopa turul olevatest dokumentide ja andmekandjate purustusseadmeid tootvatest firmadest viitab oma toodete puhul standardile DIN 32757 ning esitab vastava viite standardi turvaliigitusele ka oma toodete reklaammaterjalides ja tutvustustes.

Magnetsalvestiste kustutamist käsitleb 1993. aasta aprillist pärinev standard DIN 33858 „*Büro- und Datentechnik; Löschen von schutzbedürftigen Daten auf magnetischen Datenträgern; Löscheräte, Anforderungen und Prüfungen*“ (Büro- ja arvutitehnika. Kaitset vajavate andmete kustutus magnetilistelt andmekandjatelt. Kustutusseadmed. Nõuded ja teimid). Valdav enamik magnetilise salvestuste kustutamise seadmeid Euroopas turustavatelt firmadelt viitab oma toodete puhul sellele standardile ning esitab oma toodete reklaamides kustutusasteme vastavalt sellele standardile. Standardi olulisemate nõuete ja tehniliste detailide refereering on esitatud jaotises L 1.4.

Suurbritannias on peale selle üsna levinud Briti standard SEAP 8500, mis on koostatud 1997. aasta juunis. SEAP 8500 määratleb magnetilise kustutuse kaks taset. Taset 1 (*type 1, lower*) kasutatakse tavaliste andmete korral, taset 2 (*type 2, higher*) aga konfidentsiaalset teavet sisaldavate andmete kustutamisel. Taseme 2 puhul on nõutav kustutusugevus vähemalt 90 dB. Üldiselt kasutatakse standardit SEAP 8500 vaid Suurbritannias ning see on klassifikatsiooni ja nõuete poolest väga sarnane Saksa standardiga DIN 33858, seetõttu ei ole käesolevas ülevaates SEAP 8500 põhjalikku analüüsi esitatud.

L 1.2. PURUSTITE KLASSIFITSEERIMISE STANDARDID DIN 32757-1 JA DIN 32757-2

Standard DIN 32757 koosneb kahest osast. Standardi esimeses osas DIN 32757-1 "*Büro- und Datentechnik — Vernichten von Informationsträgern — Teil 1: Anforderungen und Prüfungen an Maschinen und Einrichtungen*" [2] on esitatud klassifitseerimis põhimõtted, mille alusel saab purustatud infokandjate tükkide suuruse

järgi jagada kõik purustid viide klassi. Esitatud on ka põhjalik teimimismetoodika purustite liigitamiseks mitmesuguste infokandjate jaoks selle klassifikatsiooni alusel.

Standardi teine osa DIN 32757-2 "*Büro- und Datentechnik; Vernichten von Informationsträgern; Maschinen und Einrichtungen; Mindestangaben*" [3] sätestab andmed, mis tuleb teimimisel iga purustimudeli kohta esitada vastavalt standardi esimeses osas 32757-1 olevale klassifikatsioonile ja metoodikale. DIN 32757-2 sisaldabki endas peamiselt andmikuvormi, millesse need andmed saab kanda. Selle vormi täielik tõlge saksa keelest on esitatud jaotises L 1.3.

Standardis sätestatud purustite viis turvataset sisaldavad endas järgmisi nõudeid:

- **Turvatase 1. Purustatud materjali tükid ei tohi olla suuremad kui 2000 mm².** Tükkide laius ei tohi olla suurem kui 12 mm, pikkus ei ole piiratud.
- **Turvatase 2. Purustatud materjali tükid ei tohi olla suuremad kui 800 mm².** Tükkide laius ei tohi olla suurem kui 6 mm, pikkus ei ole piiratud.
- **Turvatase 3. Purustatud materjali tükid ei tohi olla suuremad kui 320 mm².** Tükkide laius ei tohi olla suurem kui 4 mm, pikkus mitte suurem kui 80 mm. **Kui purustatavaks materjaliks on suure tihedusega infokandja** (nt mikrofilm, kiipkaart), sh ka digitaalne andmekandja, **ei tohi purustatud materjali tükid olla pindalalt suuremad kui 1 mm².**
- **Turvatase 4. Purustatud materjali tükid ei tohi olla suuremad kui 30 mm².** Tükkide laius ei tohi olla suurem kui 2 mm, pikkus mitte suurem kui 15 mm. **Kui purustatavaks materjaliks on suure tihedusega infokandja** (nt mikrofilm, kiipkaart), sh ka digitaalne andmekandja, **ei tohi purustatud materjali tükid olla pindalalt suuremad kui 0,5 mm².**
- **Turvatase 5. Purustatud materjali tükid ei tohi olla suuremad kui 10 mm².** Tükkide laius ei tohi olla suurem kui 0,8 mm, pikkus mitte üle 13 mm. **Kui purustatavaks materjaliks on suure tihedusega infokandja** (nt mikrofilm), sh ka andmekandja, **ei tohi purustatud materjali tükid olla pindalalt suuremad kui 0,2 mm².**

Seega on Turvatasemete 1 ja 2 nõuded DIN 32757 järgi ühesugused nii paberdokumentidele kui ka andmekandjatele. Seevastu turvatasemete 3–5 nõuded on paberdokumentide ning andmekandjate korral tunduvalt erinevad: **andmekandjatele** (ning teistele suure tihedusega infokandjatele) **kehtivad paberdokumentidest palju rangemad nõuded.**

Standardi DIN 32757 järgi testitud purustil fikseeritaksegi testimisel turvatasemed mitmesuguste materjalide puhul ning need on üldiselt eri materjalide kohta erinevad.

L 1.3. PURUSTI ANDMIK DIN 32757-2 JÄRGI

Standard DIN 32757-2 nõuab purusti turvaseme testimisel vastavalt standardile DIN 32757-2 alljärgneva andmikuvormi täitmist.

Kaitset vajavat informatsiooni sisaldavate infokandjate hävitamiseks määratud masinate ja seadmete (paberipurustite) minimaalnäitajad (DIN 32757 osa 2 järgi)

A 1. Üldandmed

A 1.1. Toode (Valmistaja/Ettevõtte) ja Mudel/Teostus

A 1.2. Tehnilised protsessid, mille kohaselt see masin või seade töötab

A 1.3. Turvaaste, DIN 32757 osa 1 järgi, millele vastab see masin või seade (märkida ristiga)

Infokandja	Infokandja hävitamise turvaaste				
Paber					
Polüesterkile algsuuruses infoesitusega					
Metall, näiteks trükivorm					
Plastik, tavaliselt kihiline, näiteks ID-kaardid					
Polüesterkile vähendusliku infoesitusega, näiteks mikrofilm					

A 1.4. Hävitatava infokandja olek, kuju, maksimaalsuurus, kogus.

Arvestades DIN 32757 osas 1 esitatud nõudeid (kanda sisse vastavad andmed):

Infokandja liik	Olek, kuju, suurus	Kogus

A 1.5. Infokandja olek, kuju, suurus pärast hävitamist (kanda sisse vastavad andmed, näiteks: korrapäratud materjaliosakesed, korrapärased materjaliosakesed, ribad, peenestatud tuhk)

Infokandja liik	Olek, kuju, suurus
Paber	
Polüesterkile algsuuruses infoesitusega	
Metall, näiteks trükivorm	
Plastik, tavaliselt kihiline, näiteks ID-kaardid	
Polüesterkile vähendusliku infoesitusega, näiteks mikrofilm	

A 1.6. Nimijõudlus ¹⁾

Korratavate jõudlusandmete saamiseks võetakse aluseks pakk standardile DIN 19307-SM4a-70 vastava paberi vinnastatud lehti.

Maksimaalarv lehti, mis pannakse käsitsi korruga masinasse või seadmesse, nii et seejärel ei tule nende hävitamiseks sooritada mingeid käsitsi sooritatavaid toiminguid:
..... tk

Aeg, mis kulub selle koguse hävitamiseks ja pärast hävitamist: s.

A 2. Seadme mõõtmed, mass, paigaldus- ja käitustingimused

A 2.1. Pikkusmm. Laiusmm. Kõrgus mm. Mass kg.

A 2.2. Paigaldustingimused (näiteks tuulutus ja väljatõmme, minimaalne ruumitarve, lauaseade, põrandaseade, käitusvahendid).

A 2.3. Käitustingimused

	Minimaalväärtus	Maksimaalväärtus
Ümbrustemperatuur, °C		
Suhteline õhuniiskus, %		

A 3. Elektritoite andmed**A 3.1. Nimipinge V.****A 3.2. Võimsustarve ²⁾**

- maksimaalne käitamisel W
- ooterežiimis W

A 3.3. Voolutarve

- maksimaalne käitamisel A
- ooterežiimis A

A 3.4. Nimisagedus(ed) Hz**A 3.5. Toide**

- Võrgust sõltuv Võrgust sõltumatu

A 3.6. Võrguühendus

- Seadmel: pistikühendus püsiühendus
- Võrgupoolel: pistikühendus pistikühendus
- Ühefaasiline Mitmefaasiline
- Võrgujuhtme pikkus m.

A 3.7. Võrgukaitsmed elektrivõrgus

- Harilikud (16 A) Muud x A
- Liini automaatkaitsme lahuskarakteristik DIN VDE 0641 järgi
- Sulavkaitsme klass DIN VDE 06363 osa 1 järgi

A 3.8. Kaitseklass

- Seade kaitseklassiga I
- Seade kaitseklassiga II (kaitseisolatsioon, seetõttu kaitsejuhtmeta)

A 3.9. Ohutustingimused

A 3.9.1. Masin või seade täidab järgmiste kodumaiste ja rahvusvaheliste standardite ja eeskirjade tingimused:

A 3.9.2. Seadmel on järgmine ohutustähis:.....

A 4. Raadiohäired

A 4.1. Masin või seade täidab DIN VDE 0871 klassi B nõuded raadiohäirepinge ja häireväljatugevuse lubatavate väärtuste kohta:

- jah
- ei

A 4.2. Seadmel on järgmine raadiohäiretõrje tähis:

A 5. Mürakiirus³⁾**A 5.1. Käitamisel**

- Helivõimsuse A-tase: $L_{WA} = \dots$ dB
- Helirõhu A-tase: $L_{AS} = \dots$ dB (kiirguse väärtus töökohal)
- Impulssilisuse määr: $K_1 = \dots$ dB

A 5.2. Ooterežiimis

- Helivõimsuse A-tase: $L_{WA} = \dots$ dB
- Helirõhu A-tase: $L_{AS} = \dots$ dB (kiirguse väärtus töökohal)
- Impulsilisuse määr: $K_1 = \dots$ dB

¹⁾ Jõudlus: läbilastava materjali kogus ajaühikus. Mõõtühikud: kg/h, tk/h jne (DIN 24450 järgi).

²⁾ Seda väärtust võib kasutada orienteeriva väärtusena soojaeralduse arvutamisel.

³⁾ Mõõdeparameetrid, mõõdetuna DIN 45 635 osa 19 või DIN 45 635 osa 31 järgi. Büroo- ja arvutitehnika alal kehtib VDI 3729 leht 1.

L.1.3 MAGNETSALVESTISTE KUSTUTUSE SEADMETE KLASSIFITSEERIMISE STANDARD DIN 33858

Magnetsalvestiste kustutuse seadmete (*degausser*) klassifitseerimise standardi DIN 33858 [4] põhiosad on

- klassifikatsioon, mille alusel saab kustutuseadmeid liigitada sõltuvalt nende kustutustugevusest ja seadmega kustutatavate andmekandjate koertsitiivväljatugevusest (vt jaotis 4.2);
- meetoodika, mis võimaldab kustutusseadmeid selle klassifikatsiooni kohaselt teimida.

Kustutustugevuse järgi jagab DIN 33858 kustutusseadmed klassidesse A ja B:

- **klassi A kuuluvate seadmete kustutustugevus peab olema vähemalt 45 dB;**
- **klassi B kuuluvate seadmete kustutustugevus peab olema vähemalt 90 dB.**

Andmekandjate koertsitiivväljatugevuse järgi jagab DIN 33858 kustutusseadmed kolme klassi. Andmekandja koertsitiivväljatugevus ja kustutustugevus sõltuvad aga tugevalt üksteisest, seetõttu saab nii A- kui ka B-klassi jagada kolmeks alamklassiks:

- klassidesse A1 ja B1 kuuluvad kustutusseadmed on mõeldud kuni 350 Oe (28 kA/m) andmekandjate kustutamiseks;
- klassidesse A2 ja B2 kuuluvad kustutusseadmed on mõeldud kuni 750 Oe (60 kA/m) andmekandjate kustutamiseks;
- klassidesse A3 ja B3 kuuluvad kustutusseadmed on mõeldud kuni 5000 Oe (400 kA/m) andmekandjate kustutamiseks;

Näiteks klassi A2 tingimusi rahuldavat kustutusseadet tähistatakse: DIN 33858 — A2.

On olemas ka kustutusseadmeid, mis on väiksema koertsitiivväljatugevuse näitajaga andmekandjaid võimelised kustutama 90 dB (klassi B nõuete) ulatuses, kuid suurema koertsitiivväljatugevusega andmekandjaid vaid 45 dB (klassi A nõude) ulatuses. Sellisel juhul tähistatakse kustutusseadet kahe klassitähisega.

Näide. Seadmele kantud tähis DIN 33858 — A3 B2 näitab, et seade on võimeline kuni 750 Oe andmekandjaid kustutama 90 dB ulatuses, kuid kuni 5000 Oe andmekandjaid vaid 45 dB ulatuses.