



# Rekommenderad policy för dataradering och hantering av it-utrustning

ATEA

 blancco

ibas<sup>®</sup> | KROLL ONTRACK<sup>®</sup>

inrego



## Syftet med policyn för organisationen där den tillämpas

Att säkerställa att information och data skyddas från obehörig åtkomst när teknisk utrustning eller datamedier återanvänds inom ORGANISATIONEN, kasseras (livscykelavslut) eller på andra sätt placeras utom organisationens eller valda partners fysiska kontroll.

En vald partner kan till exempel vara ett leasingföretag som äger utrustningen, en outsourcingpartner som äger och/eller hanterar utrustningen eller ett professionellt ITAD-företag (IT Asset Disposal) som anlitas av organisationen.

Målet med policyn och de fastställda säkerhetsprinciperna är också att förbättra våra processer för att främja återanvändning av utrustning inom eller utanför organisationen. Organisationens mål är att förlänga utrustningens livstid genom att skapa förutsättningar att återanvända den helt eller delvis, för att på bästa sätt minimera utrustningens inverkan på miljön.

Målgrupp för policyn är It-chef, miljöchef, säkerhetschef, it-avdelning, inköpsfunktion, funktioner för administrationsupport samt enhetschef. Det här dokumentet ska användas som referens för att införa och använda miljövänliga metoder för hantering av teknisk utrustning och säker radering av organisationens information på utrustningen.

Följande fakta från en FN-rapport är exempel på information som stöder vår policy och ståndpunkt:

- Under hela livstiden för en dator står själva tillverkningen för den största energiförbrukningen (81 %), medan en mindre andel (19 %) går åt för användning av den färdiga produkten.
- Datortillverkning är mycket energikrävande: förhållandet använt fossilt bränsle/produktvikt är 11:1.
- Det går åt 1,8 ton material för att tillverka en stationär dator och en skärm.

## Sammanfattning av föreslagen policy

All teknisk utrustning ska hanteras med miljömässigt hållbara metoder i en process som uppfyller lagstiftning, regler och exportprinciper samt minimerar teknikutrustningens inverkan på miljön.

Alla typer av företagsdata på teknisk utrustning som har kapacitet för lagring eller bearbetning av information, måste raderas enligt en säker process och med certifierade och godkända dataraderingsprogram, innan utrustningen flyttas. Processen ska innefatta moment för fullständig dokumentation och spårbarhet. Det ska till exempel vara möjligt att bevisa att data på en viss hårddisk har raderats.

### Exempel på utrustning med känslig data:

- Datorer, servrar, lösa hårddiskar, kopiatorer, nätverksskrivare, nätverksfaxar, kassautrustning, mobiltelefoner
- Mobila minnesenheter (t.ex. USB-minnen, SD-kort, externa hårddiskar)
- Lagringsmedia (t. ex. cd-skivor, dvd-skivor, säkerhetskopieringsband)

### Exempel på annan teknisk utrustning:

- Bildskärm, tangentbord, dockningsstation, kablage, möss etc.

### Policyn ska tillämpas i följande situationer (listan är inte fullständig):

- Kassering eller försäljning efter uppnådd livslängd
- Återinstallation inom organisationen eller till anställda
- Återlämning av utrustning när leasingperioden är slut

Villkoret för säker radering av data på utrustning som inte ägs av organisationen, måste fastställas i ett juridiskt avtal mellan organisationen och utrustningsleverantören. Utrustning eller datamedier som inte går att radera på ett säkert sätt ska destrueras.



# 1. Inledning

## 1.1 BAKGRUND

Det är avgörande för en organisation att säkerställa miljömässigt hållbar hantering av teknisk utrustning samt förhindra obehörig åtkomst till företagsinformation och andra data när teknisk utrustning (t.ex. datorer, kopieringsmaskiner, nätverksskrivare, kassautrustning, mobiltelefoner, minnesenheter (som USB-minnen och hårddiskar) och datamedier (som cd-skivor, dvd-skivor och band) placeras utom organisationens kontroll.

Den här typen av utrustning innehåller både miljöfarligt material samt digital information från organisationen som kan vara affärskritisk, skyddad av lag, upphovsrättsskyddad, konfidentiell, privat eller licensskyddad (t.ex. programvara) eller nödvändig att skydda av andra skäl. Även information i filer som användaren tror sig ha tagit bort via ”delete” eller formatering går att återställa. Därför måste samtliga data raderas från all teknisk utrustning som kan användas för lagring och/eller bearbetning av organisationens information. Raderingen måste utföras med en säker certifierad metod innan utrustningen vidarebefordras till andra parter.

## 1.2 DEFINITIONER, AKRONYMER OCH FÖRKORTNINGAR

### Säker radering

En lösning för att med certifierad och godkänd dataraderingsprogramvara radera alla data som har lagrats på hårddiskar eller andra typer av lagringsenheter. Information som måste raderas innefattar även omfördelade, defekta sektorer samt HPA- och DCO-områden.

### Avmagnetisering

Att eliminera eller minska ett magnetfält. Avmagnetisering är ett snabbt och effektivt sätt att tömma ett helt lagringsmedium. En särskild avmagnetiseringsenhet används för raderingen.

### Destruering

Att förstöra lagringsenheten fysiskt genom att till exempel bränna upp, smälta, skära sönder, pulvrисera, borra sönder eller krossa den, så att det blir omöjligt att återställa mediets data. Destrueringsmetoderna är utformade för att förstöra mediet fullständigt och skall användas i sista hand.

# 2. Säker raderingsprocess

## 2.1 ANSVAR

Det är den definierade processägarens ansvar att verifiera att rutinerna för säker radering uppfyller de krav som definieras i detta dokument. Verifiering av processer för säker radering ska utföras åtminstone en gång per år eller närhelst nya typer av datamedier eller teknisk utrustning införs. Verifieringsprocessen ska dokumenteras.

Om en tjänsteleverantör anlitas för att utföra proceduren, måste fullständig spårbarhet krävas och organisationen måste verifiera att uppgiften har slutförts med godkänt resultat. Vid beslut om att använda säker radering eller fysisk destruering bör också miljöaspekterna beaktas. Elektroniskt avfall kan innehålla stora mängder toxiska ämnen och skall därför omhändertas på ett miljörättigt sätt.

## 2.2 VERIFIERING AV PROGRAMVARA OCH UTRUSTNING FÖR SÄKER RADERING

Alla processer för säker radering måste valideras och ska uppfylla kraven enligt detta dokument. Valideringen ska baseras på externa certifikat och godkännanden för den programvara och utrustning som används för dataförstöringen. Externa certifieringsmyndigheter är till exempel statliga certifieringsorganisationer, nationella försvarsmyndigheter som hanterar testning och godkännanden och/eller organisationer som utför allmän kriterietestning. Intern testning som baseras på grundlig analys av de raderade medierna kan också godkännas om testprocesserna uppfyller aktuella branschstandarder och om utförlig dokumentation utförs.



## 2.3 ALLMÄNNA RIKTLINJER

Skadade lagringseinheter eller datamedier måste riskbedömas i syfte att fastställa om enheterna bör raderas, destrueras, repareras eller kasseras.

I hänvisnings- och bevissyfte måste säker radering, avmagnetisering eller destruering av teknisk utrustning eller datamedier rapporteras och registreras för att spårbarhet skall kunna uppfyllas.

För leasad teknisk utrustning måste leasingavtalet innehålla alla krav för säker radering och annan hantering beroende på situation.

Viktiga frågor att beakta:

- Finns det en validerad procedur för säker radering för den specifika typen av utrustning eller det specifika mediet?
- Är utrustningen eller datamediet så defekt, så att säker radering inte är möjlig?

### **Persondatorer (laptops och stationära)**

För persondatorer är det inte nödvändigt att förstöra hårddisken fysiskt, förutsatt att den raderas med en säker metod. En persondator kan anses vara säkert raderad om den metod som användes ger bevisad borttagning av data från alla adresserbara delar av lagringseinheten. Sådan dataradering ska utföras för persondatorer som ska kasseras eller avyttras. Om avmagnetisering utförs går det inte att använda hårddisken igen. Därför används avmagnetisering normalt bara för tömning av defekta hårddiskar.

### **Serverar och lagringsutrustning**

Serverar och serverbaserade lagringssystem innehåller sannolikt en mycket stor mängd data från flera olika källor. En separat process för säker radering bör därför implementeras för varje typ av lagringssystem (t.ex. NAS, SAN) och hårddisktyp (t.ex. RAID-nivå, SCSI, ATA, SATA) som används.

### **Kopieringsmaskiner, nätverksskrivare och faxar**

Kopieringsmaskiner ansluts allt oftare till nätverket och många gånger används de även som nätverksskrivare. Alla kopieringsmaskiner, nätverksskrivare och faxmaskiner som innehåller en hårddisk innehåller sannolikt även känslig data. Även om denna information inte är direkt tillgänglig för användarna av dessa maskiner, är den potentiellt tillgänglig för reparatörer, underhållspersonal eller extern part. Alla sådana maskiner bör därför genomgå en säker dataradering, avmagnetisering eller destruering vid kassering eller avyttring.

### **Mobiltelefoner, smartphones och handdatorer**

Alla mobiltelefoner och särskilt modeller med en avancerad funktionsnivå (t.ex. smartphones) skall om möjligt säkert raderas och/eller fabriksåterställas av organisationen eller vald partner. Kom ihåg att ta ut SIM-kort ur telefonen, samt att definiera en rutin för hantering av externa minneskort i telefonen.

### **Kassasystem**

I många fall är utrustning som används vid försäljningsställen hyrda och kravet på säker radering bör därför tas upp i ett juridiskt avtal. Om utrustningen ägs av organisationen ska samma procedurer användas som för persondatorer eller serverar.

### **Flyttbara minnen (USB minnen, SD-kort och externa hårddiskar)**

Vanligt borttagna filer på flyttbara lagringseinheter kan återskapas. Dessutom är det möjligt att återskapa filer på enheter som har återformatrats genom t.ex. Microsoft Windows Format eller då kortets filsystem har skadats. Säker radering eller destruering i sista hand skall utföras.

### **Cd, dvd och optiska lagringsmedia**

Det är inte möjligt att ta bort eller rensa information på cd-skivor, dvd-skivor eller andra sorters optiska diskar på ett helt säkert sätt. Den enda godkända lösningen för säker hantering av dessa enheter är avmagnetisering följt av miljöriktig komponentåtervinning.

### **Backup-band**

Den enda godkända lösningen för säker hantering av dessa enheter är avmagnetisering följt av återanvändning eller miljöriktig komponentåtervinning.

## **2.4 SÄKER RADERINGSPROCEDUR UTFÖRD AV TREDJE PART**

Processansvarig kan välja att låta tredje part utföra säker radering och miljöriktig hantering av it-utrustning. En sådan tredje part bör vara ett professionellt ITAD-företag (IT Asset Disposal) som anlitas av organisationen. ITAD-företaget skall erbjuda tjänster kring säker hantering och säker radering av it-utrustning. Vid val av tredje part rekommenderas organisationen att genomföra en kontroll av de företag (ITAD-företag) som tillfrågas rörande säkerställda processer (ISO), säkerhet (säkerhetsklassade lokaler, val av raderingsprogramvara, säkerhetsklassad personal mm), samt undersöka företagets ekonomi. Vidare så rekommenderas att ett avtal mellan organisationen och företaget som anlitas tecknas, som säkerställer hanteringen, ansvarsfördelningen, tjänster och priser.

## **2.5 KRAV FÖR SPÅRBARHET VID REVISION**

Följande minimikrav bör uppfyllas:

Programvara som används för säker radering kan styrka att processen har fullföljts genom:

1. Serienummer, inventariemärkning och modell gällande utrustning och eller datamedia
2. Vilken raderingsstandard som har använts
3. En raderingsrapport som visar att radering har utförts enligt korrekt procedur.

Avmagnetisering och destruering skall loggas manuellt för att uppnå full spårbarhet.

### **BRANSCHRÅDET FÖR DATARADERING OCH HANTERING AV IT-UTRUSTNING**

Branschrådet för dataradering och hantering av it-utrustning består av ledande aktörer inom recycling och radering. Tillsammans har vi marknadens längsta erfarenhet och kan därför erbjuda en djup kompetens inom området. Detta har utmynnat i en föreslagen policy för fri användning av företag och organisationer.

Syftet med policyn är att säkerställa att information och data skyddas från obehörig åtkomst när teknisk utrustning eller datamedier återanvänds, kasseras eller på andra sätt placeras utom organisationens eller valda partners fysiska kontroll.

Aktörerna i branschrådet är Atea (leverantör av it-infrastruktur och it-recycling), Blancco (tjänsteleverantör för certifierad dataradering), Inrego (tjänsteleverantör inom it-skiften och it-recycling), samt Ibas (tjänsteleverantör inom dataräddning, dataradering och computer forensics).