UPPSALA
UNIVERSITET

Dnr 2014/1279

Riktlinjer för Informationssäkerhet

Hantering av utrangerad (avvecklad) IT-utrustning

Fastställda av säkerhetschefen 2014-12-08
Reviderad 2016-10-31

Innehåll

1 Inledning

Teknisk utrustning som servrar, nätverksskrivare, kopiatorer, persondatorer, bärbara datorer, smarta telefoner, läsplattor, minnesenheter, datamedia med flera digitala lagringsmedier kan innehålla skyddsvärd information. När utrustningen ska flytta mellan användare inom en institution/motsvarande, mellan institutioner/motsvarande inom universitetet, avvecklas eller avyttras (kasseras, bytas bort eller försäljas) är det viktigt att förhindra obehörig åtkomst till den skyddsvärda informationen.

Riktlinjen ska vara ett stöd i det arbetet och baseras på

- Förordningen om överlåtelse av statens lösa egendom (SFS 1996:1191)
- Förordningen om producentansvar för elektriska och elektroniska produkter (SFS 2005:209)
- Regler för försäljning av inventarier (UFV 2008/159) och regelverket för universitetets anläggningsregister
- Riktlinjer för informationssäkerhet (UFV 2010/424)
- Riktlinjer inom IT-området (UFV 2013/907)
- Riktlinjen för avfallshantering (UFV 2007/551)

2 Ansvar vid bedömning

Prefekt/motsvarande har på sin institution/motsvarande det övergripande ansvaret att bedöma om det finns risk att teknisk utrustning innehåller, eller har innehållit, *okrypterad* skyddsvärd information.

För teknisk utrustning där driften hanteras av IT-avdelningen gäller att respektive *objektägare/systemägare* – vid behov i samråd med IT-chefen – har ansvaret att bedöma om det finns risk att utrustningen innehåller, eller har innehållit, *okrypterad* skyddsvärd information.

Säkerhetschefen ansvarar för att aktuell och korrekt information om kryptering, säker radering med mera finns tillgängligt i riktlinjer, stöddokument och i Medarbetarportalen.

3 Definitioner

Skyddsvärd information. Information som omfattas av sekretess eller annars ska betraktas som konfidentiell, innehåller känsliga personuppgifter, är verksamhetskritisk, licensskyddad eller skyddad av lagar och förordningar. Ofta kallad *känslig* information.

Känsliga personuppgifter. Enligt personuppgiftslagen är känsliga personuppgifter sådana som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt personuppgifter som rör hälsa eller sexualliv.

Verksamhetskritisk information kan till exempel vara kritisk för en enskild forskare/forskargrupp, en institution/motsvarande, eller kritisk för hela universitetet – som original till avhandlingar, avtalsoriginal, data/information som samlats in över lång tid och/eller inte går att återskapa, samlad information om värdefull egendom med mera.

Okrypterad information är läsbar för alla. *Kryptering* innebär att informationen kodas så att den inte går att läsa utan en nyckel för dekryptering. Se avsnittet om kryptering och säker radering.

4 Flytt av utrustning

Flytt av utrustning omfattar ej CD, DVD eller band.

4.1 Inom institution/motsvarande

När IT-utrustning, oavsett typ, ska flytta till en annan användare eller ett annat användningsområde inom samma institution/motsvarande är det tillräckligt med en systemåterställning om inte prefekt/motsvarande bedömer att en säker radering måste ske.

4.2 Inom universitetet

När IT-utrustning, oavsett typ, ska flytta till en annan institution/motsvarande men kvarstå inom universitetet, så ska informationen raderas på ett säkert sätt.

Se avsnittet om säker radering nedan.

5 Avveckling/utrangering

5.1 Allmänt

All IT-utrustning ska hanteras enligt *riktlinjer inom IT-området,* avsnittet 4.4 ”Avveckling av IT-utrustning och IT-system”, vilket bland annat innebär att

- utrangerade enheter ska hanteras på ett sådant sätt att känslig information inte kommer i orätta händer
- utrangering ska ske på ett sätt som är korrekt ur miljösynpunkt

Säkerhetsavdelningen ska kontaktas vid hantering av utrustning från samverkan/uppdragsforskning eller annat med särskilda sekretesskrav.

Utrustning som kasseras är elektronikavfall och ska hantera enligt riktlinjen för avfallshantering. Enligt förordningen 2005:209 om producentansvar för elektriska och elektroniska produkter, ska elektronikleverantör återta utrangerad och kasserad IT-

utrustning. För att utrangerad och kasserad utrustning med informationsbärande delar ska kunna återlämnas till leverantören måste leverantören kunna visa upp en godkänd process för säker destruktion.

Om det går att demontera hårddisk, flashminne eller annan lagringsmedia från utrustningen är det enbart lagringsmedia som behöver destrueras.

5.2 Försäljning

En eventuell försäljning av utrustning ska ske enligt reglerna för försäljning av inventarier och förordningen om överlåtelse av statens lösa egendom. Det innebär att universitetet enbart får avyttra egendom som blivit obrukbar eller inte behövs i verksamheten. Den avyttring som innebär försäljning ska genomföras affärsmässigt.

5.2.1 Utrustning utan skyddsvärd information

Utrustning som prefekt/motsvarande bedömer aldrig innehållit skyddsvärd information, kan avyttras efter att lagringsmedia raderats på ett säkert sätt. Detta gäller även där lagringsmedia varit *krypterad* under hela användningstiden.

Se även avsnittet om servrar och serverbaserade lagringssystem.

5.2.2 Utrustning med skyddsvärd information

För utrustning som prefekt/motsvarande bedömer har, eller kan ha, innehållit *okrypterad* skyddsvärd information gäller följande:

- Om lagringsmedia (t.ex. hårddiskar) går att demontera kan utrustningen avyttras utan lagringsmedia, eller med nytt oanvänt media installerat.
- Smarta telefoner, plattor, USB-minnen, SSD-diskar och liknande som inte kan demonteras får inte försäljas utan ska kasseras.
- För utrustning som är en del i komplexa servermiljöer, serverbaserade lagringssystem med mera ska dessutom samråd ske med säkerhetsavdelningen innan en eventuell försäljning.

Om informationen varit krypterad anses utrustningen vara utan skyddsvärd information, se 5.2.1 ovan.

5.3 CD, DVD, band

CD- eller DVD-skivor går inte att rensa. Skivor som bedöms innehålla skyddsvärd information och inte ska arkiveras ska därför destrueras när de utrangeras.

Säkerhetskopieringsband (backupband) ska avmagnetiseras och kasseras när de utrangeras. Band ska inte försäljas.

6 Kryptering och säker radering

Kryptering är ett sätt att öka säkerheten för informationen, till exempel ett e-post meddelande eller ett dokument, genom att förvränga innehållet så att det bara kan läsas av någon med rätt nyckel för dekryptering. Det finns ett antal olika tekniker och stöd för kryptering och det är viktigt att välja en tillräckligt bra teknik för att få en ökad säkerhet.

Säker radering innebär att informationen raderas på ett sätt så att den inte går att återskapa ens med användandet av speciella återskapningsprogram.

I Medarbetarportalen under Stöd och Service, Säkerhet finns tips på lämpliga programvaror för både kryptering och säker radering och kryptering, information om möjligheterna till hårdvarubaserad kryptering, länkar till ytterligare information, samt kontaktuppgifter till säkerhetsavdelningen.

Kontakta säkerhetsavdelningen för rådgivning och hjälp rörande kryptering och/eller säker radering av olika typer av lagringsmedia.

7 Servrar och serverbaserade lagringssystem

Servrar, komplexa servermiljöer och serverbaserade lagringssystem (som SAN) innehåller ofta en stor mängd information från olika källor. Hur lagringssystemet är uppbyggt påverkar i vilken mån lagringsmedier kan raderas.

Kontakta säkerhetsavdelningen för rådgivning och hjälp rörande möjligheterna för dessa typer av teknisk utrustning.

För leasad eller hyrd utrustning, som till exempel kopiatorer, nätverksskrivare, och i förekommande fall SAN-tjänster, se avsnittet om hyrd utrustning nedan.

För försäljning, se avsnitt 5.2 Försäljning ovan.

För kassering, se avsnitt 9 Fysisk destruktion nedan.

8 Leasad/hyrd utrustning

Vid återlämning av leasad eller hyrd utrustning är det viktigt att återställning, radering av information eller destruering av lagringsmedier är tydligt reglerat i avtal med leverantören.

Avtalet ska även reglera de fall då utrustning tillfälligt återlämnas på grund av service, teknikproblem eller liknande.

9 Fysisk destruktion

Fysisk destruktion innebär att förstöra utrustningen fullständigt genom att till exempel bränna upp, skära sönder, krossa eller smälta den så att återställning av data blir omöjligt. Destrueringen är förenad med risker rörande till exempel glassplitter, gasutveckling eller eld och ska enbart utföras av behörig personal.

För de campus/intendenturområden där intendenturen har utrustning för destruering – till exempel korsstrimlande dokumentförstörare som även kan hantera CD/DVD/USB-minnen eller utrustning för avmagnetisering – kan institutionen/motsvarande vända sig dit.

Utrustning där informationen ej går att radera på grund av hårdvarufel eller liknande ska destrueras om prefekt/motsvarande bedömer att utrustningen kan innehålla eller ha innehållit skyddsvärd information.

Kontakta säkerhetsavdelningen för rådgivning och hjälp.