UPPSALA UNIVERSITET

Dnr UFV 2018/668

Säker informationshantering

Rutiner för informationssäkerhet

Fastställda av Säkerhetschefen 2018-03-23
Senast reviderade 2019-08-09

Innehållsförteckning

1 Inledning

Nedanstående rutiner är baserade på *riktlinjer för säkerhetsarbetet vid Uppsala universitet* (UFV 2009/1929) och MSB:s *föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet* (MSBFS 2016:1).

Rutinerna har fastställts i syfte att

- säkerställa att all informationshantering svarar mot universitetets krav på god informationssäkerhet
- ge råd och stöd till enskilda medarbetare och prefekter eller motsvarande i samband med att enskilda medarbetare överväger att använda molntjänster
- visa på betydelsen av att informationsklassificeringar och kravanalyser genomförs i all verksamhet där information hanteras

Universitetets arbete med informationssäkerhet bedrivs i enlighet MSB:s föreskrifter om statliga myndigheters informationssäkerhet och svensk standard *SS-ISO/IEC 27001*. Nämnda standard ligger till grund för universitetets riktlinjer för informationssäkerhet och även för det material som tagits fram för genomförande informationsklassificering och kravanalys.

Informationshantering kan i många fall påverkas även av juridiska aspekter. Detta dokument avser att avgränsat hantera informationssäkerhetsmässiga aspekter.

Rutiner under punkten 4.2, Användning av molntjänster, ersätter tidigare regelverk för *Medarbetares användning av molntjänster (UFV 2015/401).*

2 Ansvar

2.1 Efterlevnad

Ansvaret för efterlevnad av dessa rutiner fördelar sig enligt följande:

Prefekt/motsvarande vid sin institution, avdelning eller motsvarande.

Områdesföreståndare för samordning inom sitt intendenturområde.

Systemägare, e-områdesansvarig/motsvarande för att följa rutinerna i utvecklings- och förvaltningsarbete samt driftuppdrag. Ansvar för efterlevnad gäller även då annan intern eller extern part anlitas för uppdraget. Utförande parts ansvar ska i förekommande fall regleras i ett s.k. servicenivåavtal.

Säkerhetschef för planering, samordning och uppföljning samt kontroll av efterlevnad.

Verksamma vid universitetet för att följa rutinerna.

2.2 Uppdatering av rutinerna

Säkerhetschefen ansvarar för att rutinerna kontinuerligt uppdateras och att underliggande stöddokument fastställs.

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.

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 visas i klartext. *Kryptering* innebär att informationen kodas så att den bara är läsbar för de som har aktuell krypteringsnyckel.

Personuppgifter. All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet räknas enligt dataskyddsförordningen (GDPR) som personuppgifter. Även bilder (foton) och ljudupptagningar på individer som behandlas i dator kan vara personuppgifter även om inga namn nämns. Krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis IP-nummer, räknas som personuppgifter om de kan kopplas till fysiska personer.

Känsliga personuppgifter. Med känsliga personuppgifter avses uppgifter om

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter och
- biometriska uppgifter som entydigt identifierar en person.

Genetiska uppgifter är personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken, vilka till exempel kan framgå av en dna-analys.

Biometriska uppgifter är personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken som erhållits genom en särskild teknisk behandling, till exempel fingeravtrycksuppgifter.

Informationsklassificering (informationsklassning) utgör ett grundläggande moment där den information som hanteras, exempelvis i ett IT-system, bedöms utifrån aspekterna konfidentialitet, riktighet och tillgänglighet.

Kravanalys. Ett moment där resultatet från genomförd informationsklassificering mappas mot det eller de system som är aktuella i sammanhanget, i syfte att säkerställa att systemet/en lever upp till en tillräcklig nivå av säkerhet med utgångspunkt från den information som hanteras i detta/dessa.

Riskhantering. Metoder för att identifiera eventuella risker och planera för riskreducerande åtgärder. I *Riskhantering av informationssystem – Rutiner för informationssäkerhet* (UFV 2018/211) beskrivs de metoder för riskhantering som används vid Uppsala universitet. Rutinerna inkluderar bl.a. stöd för genomförande av momenten *informationsklassificering* och *kravanalys*.

4 Omfattning

4.1 Information i IT-system och lagringslösningar

Nedanstående gäller samtliga IT-system och lagringslösningar som används för hantering av universitets information. Rutinerna gäller såväl för centrala lösningar som för lösningar som tillhandahålls av intendenturer eller institutioner/motsvarande.

Grunden för säker informationshantering läggs genom att en informationsklassificering genomförs – en aktivitet där informationens skyddsvärde avgörs med utgångspunkt från aspekterna konfidentialitet, riktighet och tillgänglighet. Resultatet från genomförda informationsklassificeringar med tillhörande kravanalyser anger vilka skyddskrav som bör ställas på de system/lagringslösningar som används i verksamheten.

Informationsklassificeringar och kravanalyser riktade mot universitetets centrala system (Raindance, Primula, Uppdok m.fl) genomförs inom ramen för det arbete som bedrivs i universitetets e-förvaltningsorganisation. Institutioner/motsvarande och intendenturer ansvarar för att genomföra motsvarande arbete för lokalt anskaffade system.

Material för genomförande av informationsklassificering och kravanalys har tagits fram centralt av universitetets informationssäkerhetssamordnare, som också kan bistå med hjälp vid genomförande.

Rutiner och stöd för genomförande av momenten informationsklassificering och kravanalys återfinns i *Riskhantering av informationssystem – Rutiner för informationssäkerhet* (UFV 2018/211).

Ett system som ännu inte varit föremål för en kravanalys kan anses uppfylla klassningsnivån **111** i enlighet med beskrivning i *Riskhantering av informationssystem*.

4.2 Användning av molntjänster

4.2.1 Allmänt

Molntjänster innebär att lagring, funktioner, programvara, datorkapacitet eller liknande tillhandahålls av leverantörer som tjänster över Internet. Det finns tjänster som främst är för kommersiellt bruk och sådana som är för privat bruk. Ibland kan gränserna mellan dessa vara oklara, speciellt då det gäller sådana som är allmänt tillgängliga utan direkt kostnad för den enskilde.

Det finns i detta sammanhang anledning att ange vad som skiljer en molntjänst från s.k. outsourcing där man upphandlar ett driftuppdrag eller en tjänst av något slag. I de nedanstående punkterna beskrivs den avgörande skillnaden mellan molntjänst och s.k. outsourcing:

- Avtalsmodellen är omvänd vid molntjänst jämfört med outsourcing. Vid molntjänst kan beställaren i regel inte påverka avtalet utan har att acceptera leverantörens avtal. Outsourcing innebär att kunden ska genomföra en traditionell kravställning som speglas i ett avtal som överenskommits med leverantören.
- Ytterligare parametrar som utmärker molntjänsten gentemot outsourcing är:
    - Självbetjäning (On-Demand self-service)
    - Generell tillgänglighet över nätverk (Broad network access)

Nedanstående rutiner gäller avgränsat för molntjänster enligt definition ovan. För rutiner gällande outsourcad drift – se rutiner för *anskaffning och drift UFV 2016/1944*, avsnitt 4.1.

Antalet molntjänster ökar stadigt och det finns många fördelar med molntjänster för flexibel lagring och delning av information, resurssnål IT-drift, tillgänglighet med mera. Samtidigt finns en osäkerhet runt vad som är lämpligt eller lagligt att lägga ut i molnet. Molntjänster tillhandahålls ofta av internationella företag som lyder under andra länders lagstiftning, och information som hanteras i molnet kan i praktiken hanteras i många olika länder.

För att veta hur informationen ska skyddas är det nödvändigt att veta vilken information som faktiskt hanteras och utifrån vilka aspekter det finns krav på informations-hanteringen. Momentet informationsklassificering och kravanalys, se punkten 4.1 ovan, blir av stor vikt i bedömningen huruvida det är lämpligt att använda sig av en molntjänst i det aktuella fallet.

Syftet med dessa rutiner är att ge råd och stöd till enskilda medarbetare och prefekter eller motsvarande i samband med att enskilda medarbetare överväger att använda molntjänster. För övrig användning av molntjänster, exempelvis vid anskaffning av system eller drift, finns i separata riktlinjer - se Medarbetarportalen under Stöd och service, Säkerhet.

4.2.2 Olika typer av molntjänster för enskilt bruk

Gemensam lagring

En tjänst som används för att lagra filer (dokument, ljud, bild, video med mera) och som är åtkomlig via Internet. Det finns både gratistjänster (företrädesvis för privat bruk) och betaltjänster. Huvudsyftet med dessa tjänster är att ha en plats för gemensam lagring med andra eller för att praktiskt komma åt sina filer varsomhelst.

Ett annat syfte kan vara att undvika att skicka stora filer som bilagor till e-post utan istället hänvisa till gemensam lagring. Om nyttjarna sitter geografiskt utspritt är detta en vanlig metod.

Programvaror

Tjänster där man kommer åt vissa typer av programvara utan att ha dem installerade lokalt på sin egen dator. Oftast är detta olika typer av prenumerationstjänster. Det kan vara tjänster för ordbehandling, kalkylering, presentationer, bildredigering, enkäter med mera. Även möjligheten till större processorkraft för t ex simuleringar eller bild-rendering finns som tjänster.

Webbplatser

Internetplatser för att publicera och dela information med varandra, som t.ex. sociala media, bloggar och wiki.

4.2.3 Krav på dig som användare

Molntjänster ställer krav på dig som användare att ha överblick över vilken typ av information som du, din grupp, ditt projekt, din enhet eller motsvarande har tänkt att hantera i molntjänsten, hur skyddsvärd informationen är och på vilka olika sätt den ska hanteras och kunna nås. Kryptering kan vara ett sätt att skydda informationen.

I de fall informationen bedöms vara kritisk eller väsentlig för verksamheten, eller där informationen varken får förloras, komma på avvägar eller användas av någon obehörig, ska försiktighet råda i användandet av molntjänster.

Att molntjänster inte ska användas för hantering av känsliga personuppgifter eller sekretessbelagd information utgör en grundregel i sammanhanget. Den huvudsakliga grunden för denna princip utgörs av att det vanligen är mycket svårt att säkerställa kravuppfyllnad för denna typ av tjänster. I ett fall då man, efter noggrann prövning, gör avsteg från nämnda grundregel ska beslut och motivering till detta beslut dokumenteras.

För molntjänster som man ansluter till genom att enbart ”sätta en bock i rutan” för godkännande av villkor, erbjuds ytterst sällan möjligheter till att genomföra en fullständig kravanalys. Utgångsläget för denna typ av molntjänster är därför att de inte

kan anses uppfylla en högre klassningsnivå än 111, detta enligt den princip som anges under punkten 4.1 ovan.

Personuppgifter i molntjänster

Universitetet är ansvarigt för hanteringen av personuppgifter även om någon annan part (som en molntjänstleverantör) hanterar dem på universitetets uppdrag. Som person-uppgift räknas alla uppgifter som direkt eller indirekt kan användas för att identifiera en individ.

Om personuppgifter ska behandlas, t.ex. lagras eller bearbetas, måste det säkerställas att behandlingen är tillåten enligt gällande lagstiftning, och vilka säkerhetsåtgärder som måste vidtas för att skydda personuppgifterna.

Det övergripande ansvaret för detta har prefekt, ansvarig chef eller liknande, men den enskilde medarbetaren har alltid ett eget ansvar för vad man lagrar i molntjänsten.

Inloggning, lösenord och användarprofil

Om molntjänsten inte går att nå via universitetets gemensamma webbinloggning (CAS) utan kräver att en egen användarprofil skapas för molntjänsten, ska inte samma användarkonto eller lösenord användas som används i den gemensamma webb-inloggningen.

Användare ska följa universitetets riktlinjer för lösenordshantering även vid användandet av molntjänster. Riktlinjerna för lösenordshantering finns i Medarbetarportalen, , under Stöd och Service, Säkerhet, rubriken Informationssäkerhet och IT-säkerhet[1].

Avtalsinnehåll

Molntjänstleverantörer använder oftast standardavtal lika för alla kunder/användare, avtal som är utformade på förhand med ibland liten eller ingen möjlighet att göra anpassningar. Oavsett om standardavtal eller speciella avtal används är det viktigt att kontrollera hur och på vilket sätt avtalet reglerar olika frågor.

Den som anlitar en molntjänst ska alltid läsa igenom avtalstexten innan man ansluter till den. Speciellt gäller det att kontrollera vad som gäller vid hantering av bilder då man har fotografens upphovsrätt att ta hänsyn till. I de fall avtalet innebär att moln-leverantören tar över eller delar rättigheterna till bilderna måste detta vara godkänt av upphovsmannen.

4.3 Övrig informationshantering

En stor del av den dagliga informationshantering ligger av naturliga skäl utanför de specifika system som används i verksamheten. Den kan exempelvis ingå som en del i

[1] https://mp.uu.se/web/info/stod/sakerhet/riktlinjer

rutiner och processer som omgärdar de använda systemen eller mera handla om personlig användning av olika standardprogram och lagringsmedia. Vid sidan av de krav som, utifrån genomförda kravanalyser, ställs på använda system finns riktlinjer och rutiner som behöver följas i denna informationshantering.

I universitetets mål- och regelsamling[2] återfinns övergripande *rutiner för informationssäkerhet* (UFV 2017/93) . I mål- och regelsamlingen finns även riktlinjer för hantering av allmän handling och rutiner som beskriver korrekt informationshantering på en mer detaljerad nivå.

I medarbetarportalen under Stöd och Service, Säkerhet, rubriken Informationssäkerhet och IT-säkerhet, finns länkar bland annat till riktlinjer/rutiner för lösenordshantering och säkrare elektronisk kommunikation.

4.3.1 Allmänt

Informationens skyddsvärde behöver bedömas även för den information som hanteras utanför centrala och lokala system. Informationsklassificeringar som genomförs i olika delar av organisationen, exempelvis vid institutioner/motsvarande, behöver omfatta all information som hanteras i sammanhanget.

4.3.2 Kommunikation och lagring av information

Information ska, även när de hanteras utanför centrala och lokala system, kommuniceras och lagras på ett sätt som motsvarar skyddsbehovet. I avsnittet 4.4 nedan, *Regler för säker informationshantering*, anges vilket skydd som bör omge information med olika grad av känslighet vad avser aspekterna *konfidentialitet*, *riktighet* och *tillgänglighet*.

I dagsläget är tillgången på universitetsgemensamma tjänster för lagring och delning av information begränsad. Flertalet av universitetets intendenturer och ett antal institutioner/motsvarande erbjuder tjänster för denna typ av hantering. Den organisatoriska enhet som driver och erbjuder en tjänst för kommunikation och lagring ansvarar också för att bedöma säkerhetsnivån i denna.

4.3.3 Eget ansvar/personligt förhållningssätt

Den säkerhet som omgärdar vår information är inte starkare än den svagaste länken. Information som bedömts som känslig då säkerheten i ett system bedömts, behöver omgärdas av ett fullgott skydd i all hantering.

Nedan anges ett antal punkter att ta fasta på för var och en som i sin tjänsteutövning hanterar information som bedömts vara känslig ur någon aspekt:

- Personlig utrustning som används för hantering och lagring av information ska skyddas för åtkomst och hållas under god uppsikt

[2] http://regler.uu.se

- Programvara i IT-enheter, såsom persondatorer, smarta mobiltelefoner etc., som används för hantering av information ska hållas uppdaterad
- IT-enheter ska vara försedda med automatisk skärmsläckare/låsning.
- Vid lagring på USB-minne bör informationen lagras i krypterad form,
- Enheter som används i öppna kontorsmiljöer ska låsas då de lämnas utan uppsikt
- Även icke-digital information ska omgärdas av ett skydd som motsvarar informationens känslighet – se punkten 4.3.4 nedan.

Universitetets informationssäkerhetssamordnare erbjuder regelbundet kurser i informationssäkerhet. Dessa kurser sätter ett tydligt fokus på personlig hanteringen av information och hantering av egen utrustning. Mer information finns i Medarbetarportalen under Stöd och service, Säkerhet och rubriken Utbildning.

4.3.4 Icke-digital information

Vid Uppsala universitet ska all information hanteras på ett säkert och effektivt sätt. Informationssäkerheten omfattar universitetets alla informationstillgångar oavsett om de behandlas manuellt eller med hjälp av IT, i vilken form eller miljö som de än förekommer.

Det är centralt att hitta en rimlig och väl avvägd säkerhetsnivå i den aktuella verksamheten. I öppna kontorsmiljöer är detta en utmaning. Utgå ifrån vilken typ av information som du hanterar och hur du bäst skyddar den i din miljö! Förutsättningarna är olika utifrån den fysiska miljön.

Pappersdokument, magnetband, bildmaterial och liknande kan innehålla personliga, känsliga och konfidentiella uppgifter och ska därför hanteras med utgångspunkt från hur den aktuella informationen är klassificerad.

Förvaring och hantering

För information där konfidentialitetsaspekten klassificerats till nivå 2 eller 3 ska lämpliga skyddsåtgärder införas, till exempel kontorsrum med begränsat tillträde som hålls låst när det är obemannat, eller förvaring i låsbart skåp.

Skriftligt material som innehåller konfidentiell information ska inte ligga framme så att obehöriga kan läsa den. Materialet ska hanteras så att obehöriga inte kan få tillgång till det. Tillämpa principen ”Clear desk” – lämna inte känsligt material öppet och tillgängligt. Kom ihåg att det även gäller anteckningar och post-it lappar.

Se till att du har kontroll på känsliga dokument du bär med dig utanför kontorsmiljön.

Destruktion

Pappersdokument som innehåller konfidentiell information ska vid kassering strimlas med s.k. korsstrimling eller destrueras på annat säkert sätt. För övriga media gäller rutiner som omnämns i *Hantering av utrangerad (avvecklad) IT-utrustning* (Dnr 2014/1279), avsnitt 5.3.

4.4 Regler för säker informationshantering

För information om aspekterna konfidentialitet, riktighet och tillgänglighet samt förekommande klasser – se *Riskhantering av informationssystem – Rutiner för informationssäkerhet* (UFV 2018/211).

4.4.1 Konfidentialitet

Regler klass 0
(Publik information).

- Informationen får lagras på arbetsstationens lokala hårddisk, filserver och flyttbart medium utan restriktioner. För bedömning om det dessutom är lämpligt att lagra informationen i en molntjänst - se punkten 4.2, Användning av molntjänster, eller kontakta universitetets informationssäkerhetssamordnare för vägledning.
- Informationen får överföras elektroniskt, exempelvis via e-post eller webb, utan kryptering.
- Informationen får göras tillgänglig för extern åtkomst.
- Informationen får sändas via fax och med post, såväl internt som externt.

Regler klass 1

- Informationen får lagras på arbetsstationens lokala hårddisk, filserver och flyttbart medium utan restriktioner. För bedömning om det dessutom är lämpligt att lagra informationen i en molntjänst - se punkten 4.2, Användning av molntjänster, eller kontakta universitetets informationssäkerhetssamordnare för vägledning.
- Informationen får överföras elektroniskt, exempelvis via e-post eller webb, utan kryptering.
- Informationen får göras tillgänglig för extern åtkomst med identifiering av användare.
- Informationen får sändas via fax och med post, såväl internt som externt.

Regler klass 2

- Informationen får lagras på arbetsstationens lokala hårddisk eller flyttbart medium under förutsättning att enheten hanteras i enlighet med anvisningar i avsnittet 4.3.3, *Eget ansvar/personligt förhållningssätt.* Därtill får informationen, under vissa förutsättningar, lagras i molntjänst. För bedömning om det är lämpligt att lagra informationen i en molntjänst - se punkten 4.2,

Användning av molntjänster, eller kontakta universitetets informationssäkerhetssamordnare för vägledning.

- Informationen får lagras på en filserver placerad i ett serverrum med accesskontroll.
- Informationen skall vid elektronisk överföring, exempelvis via e-post eller webb, krypteras innan den överförs externt (utanför universitetet).
- Informationen får göras tillgänglig för extern åtkomst endast via VPN-lösning eller motsvarande.
- Informationen får sändas via fax och med post, såväl internt som externt.
- Vid byte av hårddisk skall all information på den utrangerade skrivas över på sådant sätt att den inte kan återskapas.

Regler klass 3

- Informationen får lagras på arbetsstationens lokala hårddisk eller flyttbart medium under förutsättning att enheten inte lämnar universitetets lokaler och hanteras i enlighet med anvisningar i avsnittet 4.3.3, *Eget ansvar/personligt förhållningssätt.*
- Informationen får lagras på en filserver placerad i ett serverrum med accesskontroll.
- Informationen skall vid elektronisk överföring, exempelvis via e-post eller webb, krypteras innan den överförs internt eller externt.
- Informationen får göras tillgänglig för extern åtkomst endast via VPN-lösning eller motsvarande.
- Informationen får sändas med post, såväl internt som externt.
- Utbytt hårddisk får inte återanvändas utan ska destrueras enligt *rutiner för utrangerad utrustning* (UFV 2014/1279).

4.4.2 Riktighet

Se regler i avsnittet 4.4.1, Konfidentialitet. För aspekten riktighet gäller motsvarande regler som konfidentialitetsaspekten med undantag för angivna krav på kryptering, krav på VPN-lösning/motsvarande och regler vid utbyte av hårddisk.

4.4.3 Tillgänglighet

Tillgänglighetsaspekten för information som hanteras utanför centrala och lokala system handlar till stor del om säkerhetskopiering – att försäkra sig mot informationsförlust i ett fall då informationen lagras på en arbetsstations lokala hårddisk alternativt på flyttbart medium i anslutning till denna. I dessa fall ansvarar innehavaren av den aktuella utrustningen att tillse att säkerhetskopiering sker med relevant periodicitet och på ett säkert sätt enligt *Riktlinjer inom IT-området* (UFV 2016/896). Detta gäller oavsett hur informationen klassificerats med avseende på tillgänglighet, d.v.s. kravet på säkerhetskopiering gäller lika för klasserna 0-3.

Tjänster för säkerhetskopiering erbjuds i många fall av funktioner vid intendenturer och institutioner. Det åligger varje enskild medarbetare att hålla sig informerad vad gäller funktionen och omfattningen av de tjänster som används.