Dnr UFV 2018/668

UPPSALA
UNIVERSITET

Säker informationshantering

Rutiner för informationssäkerhet

Fastställda av Säkerhetschefen 2018-03-23
Senast reviderade 2022-12-15

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 informationssäkerhet för statliga myndigheter* (MSBFS 2020:6).

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 och* SS-EN ISO/IEC 27002. Nämnda standarder 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 och andra externa IT-tjänster, 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 *Rutiner för riskhantering - informationssäkerhet* (UFV 2018/211) beskrivs de metoder för riskhantering som används vid Uppsala universitet. Rutinerna inkluderar bl.a. stöd för genomförande av *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 riskbedömningar och kravanalyser anger vilka skyddskrav som bör ställas på de system/lagringslösningar som används i verksamheten.

Informationsklassificeringar och kravanalyser riktade mot universitetets centrala system (Studium, Raindance, Primula, Ladok, Medarbetarportalen 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.

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

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

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

4.2 Användning av molntjänster och andra externa IT-tjänster

4.2.1 Allmänt

Det blir allt vanligare att företag och myndigheter använder sig av molntjänster och andra typer av externa IT-tjänster. Fördelarna är många och leder ofta till en resurssnål IT-drift med ökad tillgänglighet och flexibilitet för den som använder sig av tjänsten. Samtidigt finns en osäkerhet runt vad som är lämpligt eller lagligt att lägga ut i IT-miljöer som ligger utanför den egna IT-miljön. 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.

Att finna en entydig definition av vad som ryms i begreppet molntjänst och vad som distinkt skiljer just molntjänster från andra externa IT-tjänster och s.k. outsourcing är knappast möjligt. Det har under senare år skett en förskjutning av begreppet och hur det används gentemot tidigare gjorda definitioner. I den dialog som idag pågår inom offentlig sektor och i samhället i stort används ofta begreppet molntjänst som ett mångfacetterat samlingsbegrepp. Fortsatt i detta avsnitt används uttrycket *externa IT-tjänster* som ett sådant samlingsbegrepp.

Då det kommer till informationssäkerhetsmässiga aspekter blir det mindre viktigt med definitioner som skiljer olika externa IT-tjänster från varandra. Att använda sig av en leverantörs tjänster för lagring, funktioner, datorkapacitet eller liknande och där dessa helt eller till delar finns utanför universitetets interna IT-miljö ställer särskilda krav i samband med anskaffning och användning. Detta gäller oavsett vilken benämning som används för denna företeelse - den informationssäkerhetsmässiga hanteringen blir alltid densamma vid nyttjande av externa IT-tjänster.

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

Se även rutiner för *anskaffning och drift (UFV 2020/2599)*, avsnitt 4.1.

4.2.2 Krav på dig som användare

Användning av externa IT-tjänster 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 tjänsten, hur skyddsvärd informationen är och på vilka olika sätt den ska hanteras och kunna nås.

Frågan angående huruvida det är lämpligt att använda sig av en extern IT-tjänst behöver prövas vid varje unikt tillfälle. Universitetets rutiner för *anskaffning och drift* (avsnitt 4.1) visar på moment som alltid ska genomföras i samband med anskaffning av externa IT-tjänster. Moment som genomförande av informationsklassificering/kravanalys, dialog med juridiska avdelningen, säkerhetsavdelningen och universitetets

dataskyddsombud är centrala i sammanhanget. I ett fall då man överväger att använda externa IT-tjänster för hantering av känsliga personuppgifter eller sekretessbelagd information blir dessa moment av särskilt vikt. Bristfällig eller felaktig hantering av känslig information kan utgöra lagbrott samt därtill leda till allvarliga informationssäkerhetsmässiga incidenter.

För IT-tjänster som man ansluter till genom att enbart godkänna leverantörens standardvillkor erbjuds ytterst sällan möjligheter till att genomföra en fullständig kravanalys. Utgångsläget för denna typ av tjänster 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 externa IT-tjänster

Universitetet är ansvarigt för hanteringen av personuppgifter även om någon annan part hanterar dem på universitetets uppdrag. Som personuppgift 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 också ett eget ansvar för vad man lagrar i externa IT-tjänster.

Inloggning, lösenord och användarprofil

Om den aktuella tjänsten inte går att nå via universitetets gemensamma webbinloggning utan kräver att en egen användarprofil skapas unikt för tjänsten, ska inte samma användarkonto eller lösenord användas som används i den gemensamma webbinloggningen.

Användare ska följa universitetets rutiner för lösenordshantering även vid användandet av externa IT-tjänster.

Avtalsinnehåll

Leverantörer av IT-tjänster använder ofta 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 specifika avtal används är det viktigt att kontrollera hur och på vilket sätt avtalet reglerar olika frågor.

Den som anlitar en extern IT-tjänst 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 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 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[1] finns riktlinjer för hantering av allmän handling, övergripande *rutiner för informationssäkerhet (UFV 2017/93)* och rutiner som beskriver korrekt informationshantering på en mer detaljerad nivå, till exempel för hantering av lösenord.

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

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

Säkerheten 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
- 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,

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

- 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.

Säkerhetsavdelningen erbjuder regelbundet kurser i informationssäkerhet, med ett tydligt fokus på personlig hanteringen av information och hantering av egen utrustning. Mer information finns i Medarbetarportalen under Din anställning, Kompetensutveckling, Kurser för alla, Säkerhetsfrågor.

4.3.4 Icke-digital information

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

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* (UFV 2014/1279), avsnitt 5.3.

4.4 Regler för säker informationshantering

För information om aspekterna konfidentialitet, riktighet och tillgänglighet samt förekommande klasser se rutinerna för *riskhantering* (UFV 2018/211), se särskilt Bilaga 2.

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 säkerhetsavdelningen 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 eller 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 säkerhetsavdelningen för vägledning.
- Informationen får lagras i en lagringslösning som uppfyller kravanalysens nivå 1 för konfidentialitet.
- 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 säkerhetsavdelningen.
- Informationen får lagras i en lagringslösning som uppfyller kravanalysens nivå 2 för konfidentialitet.
- Informationen får överföras elektroniskt, exempelvis via e-post eller webb, utan kryptering.
- 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 hanteras i enlighet med anvisningar i avsnittet 4.3.3, *Eget ansvar/personligt förhållningssätt.* I ett fall då enheten lämnar den ordinarie kontorsmiljön ska enhetens hårddisk alternativt den känsliga informationen vara krypterad.
- Informationen får lagras i en lagringslösning som uppfyller kravanalysens nivå 3 för konfidentialitet.
- Informationen skall vid elektronisk överföring, exempelvis via e-post eller webb, krypteras innan den överförs internt eller externt.
- 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 för konfidentialitetsaspekten, dock med undantag för destruktionskravet 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.

4.5 Säker hantering av kodnycklar

Nycklar (kodnycklar/pseudonymiseringsnycklar/krypteringsnycklar) och kodlistor ska

- förvaras separat från den information som den är kopplad till,
- förvaras i så få kopior som möjligt, dock ska minst en säkerhetskopia finnas,
- förvaras i någon form av lösning som uppfyller de krav som faller ut för klassificeringsnivån 332 enligt universitetets metoder för informationsklassificering och kravanalys *,
- ska i den lösning som väljs för lagring skyddas med ett starkt lösenord (ska bestå av minst 10 tecken – varav minst en versal, minst en gemen, och antingen minst ett specialtecken eller en siffra.),
- kommuniceras på ett säkert sätt, endast till behöriga personer.