



UPPSALA  
UNIVERSITET

Dnr UFV 2016/1944

# Riktlinjer för informationssäkerhet

---

## Anskaffning och drift av IT-system

Fastställda av Säkerhetschefen 2017-01-16

# Innehållsförteckning

<b>1</b>	<b>Inledning</b>	<b>3</b>
<b>2</b>	<b>Ansvar</b>	<b>3</b>
2.1	Efterlevnad	3
2.2	Uppdatering av rutinerna	3
<b>3</b>	<b>Definitioner</b>	<b>4</b>
<b>4</b>	<b>Omfattning</b>	<b>4</b>
4.1	Säkerhetskrav vid inköp av system eller molntjänster	4
	Kravställning vid upphandling eller avrop	5
	Upprättande av servicenivåavtal (SLA)	5
4.2	Hantering av tillgångar	6
4.3	Krav på driftmiljöer	6
	Styrning av åtkomst	6
	Fysisk och miljörelaterad säkerhet	7
	Driftsäkerhet	8
	Kommunikationssäkerhet	8
4.4	Anslutning till universitetets datornät	9
4.5	Säkerhetskopiering i driftmiljöer	9
4.6	Loggning	10
	Logghantering	10
	Syslog	11
	Utlämning av loggar	11

# 1 Inledning

Nedanstående rutiner har fastställts i syfte att

- säkerställa att system och tjänster som upphandlas svarar mot universitetets krav på god informationssäkerhet
- upprätthålla en hög nivå av säkerhet i driftmiljöer och i universitetets datornät
- garantera tillgänglighet till information och system i händelse av förlust eller förvanskning av information i ordinarie lagringsmiljö eller liknande händelse
- uppnå en säker logghantering för alla servrar och annan utrustning som tillhandahåller nätverksbaserade tjänster vid Uppsala universitet
- säkerställa att personuppgifter i system och tjänster behandlas i enlighet med personuppgiftslagen

Rutinerna är ett komplement till riktlinjerna för *produktionssättning av IT-system för central användning* (UFV 2014/1171), och baseras på universitetets *riktlinjer för säkerhetsarbetet* (UFV 2009/1929), *riktlinjer inom IT-området* (UFV 2016/896) och MSB:s *föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet* (MSBFS 2016:1).

Rutinerna ersätter tidigare regelverk för *säkerhetskopiering och loggning, säkerhetskrav vid inköp av system eller molntjänster, samt användning av syslog*.

## 2 Ansvar

### 2.1 Efterlevnad

Ansvar 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

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

*Systemägare* beskriver i detta dokument den roll som har det övergripande ansvaret för förvaltning och drift av ett eller flera IT-system. Rollen e-områdesansvarig, som används inom de delar av organisationen som tillämpar universitetets e-förvaltningsmodell, innefattas i begreppet systemägare.

*Servicenivåavtal*, eller *servicenivåöverenskommelse*, är en skriftlig överenskommelse som reglerar vilka nivåer som ska gälla för exempelvis driftövervakning och support. Servicenivåavtalet reglerar även vilka rutiner som ska gälla för säkerhetskopiering och återläsning. Ansvarig för förvaltningsorganisationen och ansvarig för driftorganisationen utgör parter vid upprättande av ett sådant avtal. Ofta används uttrycket SLA (eng. *Service Level Agreement*) istället för servicenivåavtal.

## 4 Omfattning

### 4.1 Säkerhetskrav vid inköp av system eller molntjänster

Vid anskaffning av system eller molntjänst ska kraven i avsnitten nedan gällande tillgångar, driftmiljöer, nätanslutning, säkerhetskopiering och loggning beaktas. Att anlita en leverantör för ett driftuppdrag ska alltid föregås av en informationsklassificering (se 4.2, avsnittet *Hantering av tillgångar* nedan).

Om det aktuella systemet hanterar känslig information ska en riskbedömning göras innan leverantörer eller andra externa parter ges tillgång till informationen.

Om personuppgifter kommer att hanteras ska leverantören underteckna ett personuppgiftsbiträdesavtal. Notera att utöver Sverige/EU får personuppgifter överföras till de stater som anges i bilaga 1 till personuppgiftsförordningen (SFS 1998/1191), inklusive *EU - US Privacy Shield*.

Relevanta informationssäkerhetskrav ska vara fastställda i avtal med leverantören. I detta avtal ska även ett sekretessavtal ingå. All personal som hyrs in från leverantörer till systemet/systemen ska vara informerade om de säkerhets- och sekretesskrav som har avtalats.

## Kravställning vid upphandling eller avrop

När ett system eller en tjänst ska upphandlas bör följande ingå i kravställningen:

- Hur leverantören bevakar information om nya sårbarheter, följer upp dessa med avseende på driftmiljön, samt hanterar IT-säkerhetsincidenter
- Hur universitetets information skyddas från leverantörens andra kunder
- Hur kopplingar till underliggande eller angränsande system (t.ex. LTI) hanteras
- I vilket/vilka land/länder informationen lagras och hanteras, både i systemet och eventuellt underliggande system
- Krav på information i händelse av migrering av data mellan leverantör och underleverantör eller mellan länder
- Vad som gäller för eventuella integrerade system utvecklade av universitetet eller i samråd mellan universitetet och leverantören, till exempel vid uppgraderingar, för bakåtkompabilitet med mera
- Hur loggar hanteras samt ange hur universitetet vid behov kan få tillgång till loginformation
- Hur universitetet återfår sin information om/när systemet avvecklas
- Hur systemet arkiveras
- Hur ser prioriteringen ut mellan leverantörens olika kunder vid större driftavbrott

## Upprättande av servicenivåavtal (SLA)

Då ett driftuppdrag läggs ut på annan part ska ett servicenivåavtal upprättas mellan parterna. I avtalet bör bland annat framgå

- Påverkan på, och beroenden av, andra tjänster
- Vilka eventuella tredjepartstjänster som ingår i överenskommelsen
- Ansvarsfördelning mellan kund och leverantör
- Rutiner för säkerhetskopiering och för återläsning
- Rutin för återställning av tjänsten
- Avtalat tillgänglighetsfönster, d.v.s. den tid som avtalats att tjänsten ska fungera, mäts på och har support av något slag
- Överenskommen support och ärendehanteringsprocess
- Rutin för förändringshantering (problem, incident och change processer där ITIL tillämpas)
- Rutin för rapportering inklusive hur driftavbrott – planerade och oplanerade - meddelas
- Nivå för automatisk övervakning
- Kontinuitetshantering vid större driftavbrott
- Rutin för leverantörskontakter, till exempel gällande avstämningsmöten

Översyn och eventuell revision av gällande avtal ska göras årligen.

## 4.2 Hantering av tillgångar

En informationsklassificering ska alltid genomföras som ett initialt steg, oavsett om ett system produktionsätts för drift i egen regi, leverantör anlitas, eller en molntjänst avropas. Vid genomförande av en informationsklassificering bedöms informationens behov av säkerhetsmässiga åtgärder utifrån krav på tillgänglighet, konfidentialitet och riktighet.

För redan driftsatta system gäller att riskanalyser ska genomföras regelbundet enligt rutinerna för *riskanalyser av informationssystem* (UFV 2015/322), som finns i Medarbetarportalen under Stöd och service, Säkerhet. I rutinerna ingår även informationsklassificering och nulägesbedömning.

De krav som ställs på myndigheter vad gäller hantering av allmänna handlingar och personuppgifter ska följas, till exempel integritetskrav enligt personuppgiftslagen. Register som innehåller personuppgifter ska vara anmälda till universitetets personuppgiftsombud.

Molntjänster där lagring enligt personuppgiftsförordningen (se avsnitt 4.1 ovan) inte kan garanteras, ska inte användas för lagring av information belagd med sekretess eller för känsliga personuppgifter. Personuppgiftslagen definierar följande som känsliga personuppgifter: ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, personuppgifter som rör hälsa eller sexualliv.

## 4.3 Krav på driftmiljöer

### Styrning av åtkomst

Alla system bör om möjligt vara kopplade till universitetets gemensamma inloggnings-tjänst (CAS) och därtill hörande lösenordshantering. Även för övriga system ska lösenord vara utformade, hanteras och användas i enlighet med de riktlinjer för lösenordshantering (UFV 2013/1490) som gäller vid universitetet.

För att få spårbarhet ska systemanvändare ha unika användaridentiteter, dvs. inga gruppidentiteter får finnas. Undantag kan medges i specifika fall efter dialog med säkerhetsavdelningen.

En dokumenterad rutin för behörighetstilldelning och behörighetsadministration ska finnas och följas. Rutinerna för behörighetsadministration ska omfatta att medge, förändra och återkalla åtkomst till ingående information, system och tjänster. De ska också ange att tilldelning av sysadmin- och användarkonton med höga behörigheter ska begränsas, samt granskas och revideras regelbundet.

Det ska gå att begränsa användares åtkomst till system och databaser utifrån roll, organisationstillhörighet etc.

Åtkomst till tjänster och verktyg (operativsystem, nätverkstjänster, systemverktyg etc.) med möjlig påverkan på systemets säkerhet, liksom användning av verktyg (t.ex. SQL-verktyg) som kan kringgå säkerhets- och loggningsåtgärder i systemet, ska begränsas och styras strikt.

Om åtkomst till system innehållande känslig information sker på distans ska universitetets VPN-tjänster för säker internetuppkoppling användas.

Programvaruleverantörers och annan servicepersonals åtkomst till känslig information ska begränsas och vara reglerad i sekretessavtal. Kontakta säkerhetsavdelningen för hjälp med utformning av sekretessavtal.

### **Fysisk och miljörelaterad säkerhet**

Lokaler där systemets/systemens dator drift sker eller där datamedia förvaras ska vara skyddade med ett ändamålsenligt skalskydd - lås, larm, passagesystem (kort och kod) etc. för att minimera risken för obehörig åtkomst.

Särskilda skyddsåtgärder ska övervägas för lokaler som innehåller känslig eller kritisk information eller utrustning.

Endast behörig personal ska ha tillträde till berörda lokaler eller utrymmen.

Dokumenterade rutiner ska finnas och följas för tillträde till och arbete i lokalerna.

Utrustningen ska vara placerad och skyddad på ett sådant sätt att riskerna för miljörelaterade hot (temperatur, brand, vatten) minimeras. De fysiska delarna (hårddiskar, kablar, fläktar etc.) ska underhållas och uppdateras på ett korrekt sätt som säkerställer fortsatt tillgänglighet och riktighet. Dessa delar regleras i SLA.

Om systemet/systemen har höga eller särskilda krav på tillgänglighet ska avbrottsfri kraft (UPS) för dator driften finnas installerad hos driftsleverantören som även ska kunna uppvisa rutiner och dokumentation av att regelbundna tester av UPS-systemet genomförs.

Dokumenterade regler och rutiner ska finnas för fysisk transport av data, exempelvis via portabla lagringsmedia som USB-minnen och liknande.

När utrustning som kan innehålla skyddsvärd information ska flytta mellan användare inom eller mellan institutioner, eller ska avvecklas eller avyttras (kasseras, bytas bort eller försäljas) ska universitetets riktlinjer för hantering av utstrangerad IT-utrustning följas (UFV 2014/1279).

## Driftsäkerhet

En formaliserad ändringshantering (t.ex. *change management* där ITIL tillämpas) ska finnas och tillämpas av driftsleverantören avseende nya versioner av aktuella tjänster, hårdvara, systemprogramvara och operativsystem. Dessutom ska en formaliserad problem- och incidenthanteringsrutin ska tillämpas av driftsleverantören.

Utvecklings-, test- och produktionsmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i produktionsmiljöer.

Om systemet har *höga* eller *särskilda krav* på tillgänglighet ska driftsleverantören dagligen övervaka och vid behov justera kapacitetsbehovet. Leverantören ska även göra regelbundna prognoser av framtida kapacitetskrav.

Både användaraktiviteter i systemet/systemen, liksom systemoperatörers och administratörers aktiviteter, ska loggas och loggarna ska sparas på ett säkert sätt. Se avsnittet 4.6 *Loggning* nedan. Loggar och loggningsverktyg ska vara skyddade mot obehörig åtkomst och manipulation.

Systemet/systemen ska vara anslutet till en central systemklocka (ntp) för tids-synkronisering mot en och samma referenskälla. Universitetets centrala tidsservrar ska användas av de system som är anslutna till universitetets nätverk.

Säkerhetskopior av databaser, programvara och övriga kritiska funktioner eller parametrar ska tas och testas regelbundet.

## Kommunikationssäkerhet

De nätverk som används för dataöverföring ska vara uppbyggda, administrerade och övervakade av driftsleverantören på ett sätt som säkerställer tillräcklig säkerhet.

Säkerhetsåtgärder som uppfyller systemets krav på säker dataöverföring i de nätverkstjänster som används ska vara överenskomna och specificerade i avtal med driftsleverantören.

Vid överföring av känslig information till annat system, annan myndighet eller andra externa parter ska skyddsåtgärder vid bearbetning, lagring och publicering av informationen vara reglerade i avtal.

Om systemet hanterar information med höga eller särskilda krav på sekretess ska kommunikation av information ske i krypterad form.

All trafik för autentisering och all persondata ska gå krypterat.

Alla portar och protokoll systemet använder ska vara dokumenterade för att möjliggöra regler i perimeterskydd (brandväggar med mera).



## 4.4 Anslutning till universitetets datornät

Nätverksutrustning, som exempelvis routrar och switchar, får inte kopplas in på nätverket utan tillåtelse från IT-ansvarig eller den person som är ansvarig för nätverkssegmentet.

Institutionen/motsvarande ska ha en förteckning över installerad utrustning. Tillräcklig dokumentation ska finnas för att den IT-ansvarige ska kunna lokalisera ansluten utrustning. I dokumentationen ska framgå

- vem som ansvarar för utrustningen,
- syfte,
- identifikation (t.ex. MAC-adress, SSID på routers).

Endast tjänster som används, och som överensstämmer med syftet, får aktiveras på utrustningen. Tjänster som inte används ska inaktiveras.

Utrustning och all programvara ska vara uppdaterad. I den mån leverantören inte längre underhåller utrustningen får den inte anslutas till universitetets datornät. Undantag kan medges i specifika fall efter dialog med säkerhetsavdelningen.

Utrustningen ska placeras så att fysisk åtkomst är möjlig endast för behörig personal.

Router med trådlöst nätverk ska vara konfigurerad med starkast möjliga kryptering.

Om nätverksutrustningen används för lagring av känslig information ska denna vara krypterad.

## 4.5 Säkerhetskopiering i driftmiljöer

Säkerhetskopiering ska göras regelbundet och omfatta all information som är av värde för verksamheten och som är svår, kostsam eller tidsödande att återskapa.

Systemägaren ska besluta om vilken information som ska omfattas av säkerhetskopieringen, samt periodicitet för säkerhetskopiering och återläsning. Regleras i SLA.

Säkerhetskopieringen ska testas regelbundet genom återläsning. Efter återläsning ska systemtester genomföras för att säkerställa bibehållen funktionalitet i de berörda systemen. Överenskommen periodicitet för återläsning ska dokumenteras i upprättat servicenivåavtal.

Säkerhetskopior ska sparas i flera generationer så att information kan återställas även om problem uppstår med att använda den senast tagna säkerhetskopian.

Säkerhetskopior ska förvaras säkert och skilda från berörda datorer. Då informationen inkluderar delar som vid informationsklassning bedöms tillhöra nivån *särskilda krav*, ska krypterad lagring av säkerhetskopian övervägas.

Utöver de säkerhetskopior som tas regelbundet, enligt fastställd periodicitet, ska säkerhetskopiering ske före och efter genomförande av en större förändring i system eller i driftmiljö. IT-system och lagrad information ska, så långt det är möjligt, kunna återskapas på annan maskinvara.

## 4.6 Loggning

Uttrycket *Logg* syftar i detta sammanhang på kontinuerligt insamlad information om de operationer som utförs i ett system eller i ett nätverk.

*Säkerhetsloggar* används som ett samlingsbegrepp för autentiseringsloggar, trafikloggar samt andra loggar som ger spårbarhet till en enskild individ. Säkerhetsloggar sparas primärt för att användas i forensiskt syfte, bl.a. vid utredning av intrångsförsök eller fullbordat intrång.

*Applikationsloggar* används primärt som ett redskap för att spåra händelser i ett specifikt IT-baserat system. *Transaktionsloggar* eller *Systemloggar* kan användas som synonyma uttryck. För vissa typer av uppgifter, exempelvis ekonomiska transaktioner, finns lagstiftning som anger regler för hur loggning ska ske.

Nedanstående gäller för alla servrar och annan utrustning som tillhandahåller nätverksbaserade tjänster vid Uppsala universitet:

### Logghantering

Systemägare ska besluta om vilka loggar som ska sparas. Som ett minimum ska samtliga autentiseringsloggar och accessloggar från nätverksbaserade tjänster sparas.

Applikationsloggar ska sparas minst 6 månader eller under tid som lagstiftning föreskriver. Tidsrymd för sparande av applikationsloggar ska avtalas med driftsleverantören.

Vid uppdatering av information som vid informationsklassning bedöms tillhöra nivån *särskilda krav*, bör loggningen inkludera information om vem som utförde transaktionen och vad som uppdaterades.

Om uppgifter som registreras i en loggfil går att knyta till en enskild person betraktas de som personuppgifter. Det är inte tillåtet att använda loggar på ett sätt som inkräktar på den personliga integriteten för en enskild individ. Till exempel är användning av loggar för att, oavsett skäl, kartlägga en persons rörelsemönster på internet inte tillåtet.

Alla loggar ska skyddas mot obehörig åtkomst och oavsiktlig förändring samt sparas på ett säkert sätt, helst inte i omedelbar anslutning till lokalen för drift. Endast personer

som i sin tjänsteutövning kan anses ha nytta av informationen i loggarna ska ges tillgång till dem.

## Syslog

*Syslog* är en standard för sändning av loggmeddelanden. Normalt används *syslog* för övervakning av datasystem eller för audit-loggning (kronologisk sammanställning). *Syslog* kan användas för att integrera loggdata från många olika system i ett centralt lagringsutrymme på en *syslog*-server.

För serverar och annan utrustning som driftas på Uppsala universitetet gäller att samtliga loggar – säkerhetsloggar såväl som applikationsloggar – ska skickas i ett standardiserat *syslog*-format (RFC 5424) till universitetets *syslog*-server, ***syslog.uu.se***. Används egen loggserver ska denna kopiera informationen till *syslog.uu.se*.

Tänk på att vissa servrar kräver att man anger *syslog*-server med ipnummer. Kontakta servicedesk ([servicedesk@uu.se](mailto:servicedesk@uu.se)) för hjälp, t.ex. med att välja lämplig *syslog*-klient.

## Utlämning av loggar

Offentlighetsprincipen står inskriven i tryckfrihetsförordningen och innebär att var och en kan vända sig till en myndighet och begära ut en allmän handling. I begreppet allmän handling inkluderas texter, bilder, ljudinspelningar som kommit till, eller skapats på en myndighet. Även information som skapats automatiskt via IT-system, exempelvis i form av loggar, kan utgöra allmänna handlingar. Allmänna handlingar är normalt offentliga, men utlämning av en handling ska alltid föregås av en prövning.

För att säkerställa att utlämnandet av uppgifter inte riskerar att skada den personliga integriteten för en enskild individ gäller följande vid all utlämning av loggar, säkerhetsloggar såväl som transaktionsloggar:

- Begäran om utlämning av loggar, säkerhetsloggar såväl som transaktionsloggar - eller information som inkluderas i loggar, ska ställas till aktuell systemägare. Det är systemägaren som svarar för prövningen, d.v.s. bedömning av huruvida utlämning av efterfrågad information riskerar att skada den personliga integriteten för en enskild individ. Säkerhetsavdelning bistår vid behov med stöd i att identifiera berörd systemägare, liksom med stöd vid tveksamheter i prövningsfrågan. Uppgifter från universitetets passersystem som anger en persons rörelsemönster i universitetets lokaler, kameraloggar och uppgifter om en persons rörelsemönster på internet är tydliga exempel på uppgifter kopplade till personlig integritet.
- En enskild individ äger alltid rätten att begära ut sin egen information, det vill säga allt som finns vid myndigheten eller i ett visst system med identifierad koppling till den egna personen.