Dnr UFV 2014/1308

UPPSALA
UNIVERSITET

Riktlinjer för informationssäkerhet

Säkerhetskopiering och loggning

Fastställda av Säkerhetschef 2014-11-25

Innehållsförteckning

1 Inledning

Nedanstående riktlinjer har fastställts i syfte att

- garantera tillgänglighet till information och system i händelse av förlust eller förvanskning av information i ordinarie lagringsmiljö eller liknande händelse,
- uppnå en forensiskt säker logghantering för alla servrar och annan utrustning som tillhandahåller nätverksbaserade tjänster vid Uppsala universitet.

Fastställda riktlinjer gäller oavsett om driftuppdraget hanteras operativt vid den egna institutionen/motsvarande eller om det lagts ut på annan intern eller extern part. Då ett driftuppdrag läggs ut på annan part ska ett servicenivåavtal upprättas mellan parterna. Detta avtal ska bl.a. reglera vilka rutiner som ska gälla för loggning, säkerhetskopiering och återläsning. Enligt universitetets *Riktlinjer inom IT-området* ska ett servicenivåavtal upprättas före driftsättning av ett system, detta oavsett om systemet utvecklas och förvaltas inom universitetets organisation eller om det förvärvas genom upphandling.

2 Ansvar

2.1 Efterlevnad

Ansvaret för efterlevnad av dessa riktlinjer fördelar sig enligt följande:

Prefekt/motsvarande vid sin institution, avdelning eller motsvarande.

Områdesföreståndare för samordning inom sitt intendenturområde.

Systemägare, objektägare/motsvarande för att följa riktlinjerna 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 riktlinjerna.

2.2 Uppdatering av riktlinjerna

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

3 Definitioner

Systemägare beskriver i detta dokument den roll som har det övergripande ansvaret för förvaltning och drift av ett eller flera IT-system. Rollen objektägare, som används inom de delar av organisationen som tillämpar pm3-modellen, innefattas i begreppet systemägare.

Pm3-modellen är den förvaltningsstyrningsmodell som används i arbetet med att förvalta centrala administrativa system vid Uppsala universitet. Modellen ger stöd för att skapa tydliga förvaltningsuppdrag med god samverkan mellan representanter för verksamhet och IT.

Servicenivåavtal 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 istället för servicenivåavtal, vilket syftar på det engelska uttrycket Service Level Agreement. Även uttrycket servicenivåöverenskommelse kan förekomma.

Informationsklassificering utgör ett moment där information som hanteras, exempelvis av ett IT-system, bedöms utifrån aspekterna konfidentialitet (sekretess), riktighet och tillgänglighet. Informationens behov av säkerhetsmässiga åtgärder bestäms i en behovsskala bestående av nivåerna basnivå, hög nivå samt särskilda krav. Stöddokument för informationsklassificering återfinns i Medarbetarportalen under STÖD OCH SERVICE, Säkerhet, Riktlinjer och stöddokument.

4 Omfattning

4.1 Säkerhetskopiering

4.1.1 Övergripande angående säkerhetskopiering

- 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.

- 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 nyttja 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.

4.1.2 Säkerhetskopiering av persondatorer, mobil utrustning och portabla lagringsmedia

I universitetets riktlinjer inom IT-området uttrycks följande angående säkerhetskopiering av enheter som persondatorer, mobil utrustning och portabla lagringsmedia:
”Innehavaren är ansvarig för att säkerhetskopiering sker med relevant periodicitet och på ett säkert sätt. Uppdateringar, antivirus och säkerhetskopiering sköts i normalfallet av IT-ansvarig/dataansvarig på respektive institution/motsvarande eller av intendenturen. Prefekt/motsvarande kan besluta om undantag från detta.”

Det åligger innehavaren av den aktuella utrustningen att inhämta kunskap om vad som gäller vid den egna institutionen/motsvarande. Innehavaren är själv ansvarig för säkerhetskopiering som inte hanteras på ett samordnat sätt vid institutionen/motsvarande.

4.2 Loggning

Enheter anslutna till Uppsala Universitets nät är ständigt utsatta för intrångsförsök från omvärlden och i vissa fall även från vårt eget nät. För att kunna göra en samlad bedömning av storlek på intrång, hur intrånget skedde och vilken information som eventuellt kan vara komprometerad behöver loggar från, för en angripare, attraktiva slutmål sparas på ett forensiskt säkert sätt.

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

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

- Tidsrymd för sparande av transaktionsloggar (loggar som gör det möjligt att spåra händelser i ett IT-baserat system) ska avtalas med driftsleverantören. Transaktionsloggar ska sparas minst 6 månader eller under tid som lagstiftning föreskriver.

- 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.

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

- Säkerhetsloggar ska skickas i ett standardiserat syslogformat till syslog.uu.se. enligt instruktioner som återfinns i Medarbetarportalen under STÖD OCH SERVICE, Säkerhet, Riktlinjer och stöddokument. Används egen loggserver ska denna kopiera informationen till syslog.uu.se.

- All information som behövs för att identifiera användarID och IP-adress ska inkluderas i den information som skickas till syslog.uu.se

- Säkerhetsrelaterade loggar som skickas till syslog.uu.se sparas av säkerhetsenheten i 24 månader varefter de destrueras.