UPPSALA
UNIVERSITET

Dnr UFV 2018/1170

Hantering av behörigheter och roller

Rutiner för informationssäkerhet

Fastställda av Säkerhetschefen 2018-08-14

Innehållsförteckning

1 Inledning

Universitetets arbete med informationssäkerhet bedrivs i enlighet MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1) och svensk standard *SS-ISO/IEC 27001*. Att ha dokumenterade rutiner för hantering av roller och behörigheter lyfts fram som tydliga krav i dessa.

Ett flertal av de krav som finns listade i universitetets material för kravanalyser (*Riskhantering av informationssystem – Rutiner för informationssäkerhet* (UFV 2018/211), bilaga 3) har en tydlig koppling till säkerhetsåtgärder med fokus på hantering av behörigheter och roller.

Rutinerna har fastställts i syfte att säkerställa att information som betraktas som känslig utifrån aspekterna konfidentialitet och riktighet skyddas från obehörig åtkomst och obehörig förändring – detta genom att

- användare ges tillträde endast till den information och de tjänster som de specifikt givits tillträde till
- roller som i sin tur medför rättigheter är tydligt definierade
- momenten registrering och avregistrering av användare och behörigheter styrs av dokumenterade rutiner
- behörigheter hålls aktuella genom att regelbundna granskningar genomförs

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.

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

Informationssäkerhet. Säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad tillgänglighet, riktighet, konfidentialitet (sekretess) och spårbarhet.

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-förvaltnings-modell, innefattas i begreppet systemägare.

4 Omfattning

4.1 Grundläggande krav avseende hantering av behörigheter och roller

Nedanstående krav ska beaktas vid all behörighetshantering kopplad till system och tjänster som används vid Uppsala universitet.

- Behörigheter/behörighetsnivåer samt därtill ev. förekommande roller, som i sin tur medför rättigheter, ska vara tydligt definierade och dokumenterade. Dokumentationen ska hållas aktuell och uppdateras exempelvis vid eventuella förändringar i definitioner.

- Tilldelning, ändring samt borttag av behörigheter ska följa rutiner som säkerställer att förekommande behörigheter hålls aktuella. Förändringar som sker i organisationen, exempelvis genom en person byter roll alternativt avslutar sin tjänstgöring ska återspeglas i personens innehav av behörigheter.

- Den totala bilden av aktuella behörigheter i ett system ska kunna göras tydlig på ett enkelt vis för att möjliggöra fortlöpande kontroller av gällande behörigheter. Ansvaret för att praktiskt genomföra dessa kontroller ska vara tydligt delegerat. Vid sidan av de fortlöpande kontrollerna ska en större planerad behörighetsinventering genomföras minst en gång per år alternativt vartannat år beroende på systemets klassificering. En kravanalys enligt universitetets metod för kravanalysering (*Riskhantering av informationssystem – Rutiner för informationssäkerhet* (UFV 2018/211), bilaga 3) ger besked om periodicitet vad gäller den planerade behörighetsinventeringen.

- Behörigheter ska, så långt det är möjligt, vara baserade på personliga användaridentiteter. Gruppidentiteter får endast användas i undantagsfall omgärdat av en bedömning av säkerhetsmässiga konsekvenser.

- Då externa parter tilldelas behörigheter i universitetets system ska detta föregås av en riskbedömning. I ett fall då externa parter ges tillgång till känslig information ska

detta omgärdas av en restriktiv hållning samt därtill föregås av en bakgrundskontroll där samtliga aktuella personer inkluderas.

4.2 Angående dokumentation av behörigheter och roller

En dokumentation som innehåller relevant information och som uppdateras löpande utgör en nödvändighet i sammanhanget. Nedanstående punkter anger grundläggande krav och förutsättningar vad avser dokumentation av behörigheter och roller.

- Det åligger systemägare, e-områdesansvarig/motsvarande att tillse att dokumentation över behörigheter och roller upprättas och hålls aktuell.

- Information om vilka som innehar behörigheter att hantera känslig information kan i sig själv betraktas som känslig och i behov av skydd. Det är av stor vikt att dokumentationen förvaras och hanteras med hänsyn tagen till känsligheten i denna.

- Kraven på vad som behöver dokumenteras och hur dokumentationen bäst utformas skiljer sig från fall till fall. Det åligger systemägare, e-områdesansvarig/motsvarande att utforma dokumentationen i enlighet med de aktuella behoven.