Informationssäkerhetskrav riktade mot den interna organisationen

1. Inledning

I samband med anskaffning av nya system hamnar fokus av naturliga skäl på de tekniska kraven riktade mot leverantören av systemet. I regel tas dessa krav fram tillsammans med upphandlare och projektledare/motsv. i samband med upphandlingsförfarandet för att ingå i det aktuella upphandlingsunderlaget. Sådana krav utgör endast en delmängd av de krav som faller ut vid en fullständig kravanalys med hjälp av bilaga 3 till Rutiner för riskhantering (UFV 2018/211). Detta dokument har tagits fram i syfte att säkerställa att även övergripande krav och krav som riktar sig mot administrationen av de aktuella systemen inte ska tappas bort.

2. Grundläggande krav (kravkategori Policy/riktlinjer)

Alla anställda inklusive konsulter ska känna till var riktlinjer för informationssäkerhet finns med underliggande riktlinjer, anvisningar och stöddokument.

Innehavare av roller i förvaltningsorganisationen ska

- vara införstådda med sitt ansvar för informationssäkerheten i berörda system och arbeta aktivt med att initiera, stödja och följa upp säkerhetsförbättringar,
- vara införstådda med sitt ansvar att koordinera och driva arbetet med informationssäkerhet,
- via Intranätet ta del av aktuell säkerhetsrelaterad information (ex. Ledningsnytt, säkforum, driftinformation),
- känna till att IT- och informationssäkerhetsincidenter samt personuppgiftsincidenter ska anmälas till servicedesk.

Det ska för respektive system finnas ett uppdaterat utbildningsmateriel. Personal som ska använda IT-systemet ska utbildas innan de ges access till systemet.

Mobila enheter inklusive laptops ska ha skärmlås, virusskydd och uppdaterat operativsystem.

Bakgrundskontroll ska göras av sökande till anställning som innebär tillgång till särskilt känslig information.

Informationsklassning ska genomföras för all information som hanteras i verksamheten. Informationsklassning genomförs och dokumenteras när ny information ska hanteras i verksamheten.

Register som innehåller personuppgifter ska vara anmälda till verksamhetens personuppgiftsombud/dataskyddsombud.

Programvaruleverantörers och annan servicepersonals åtkomst till känslig information ska begränsas och vara reglerad i sekretessavtal.

3. Säkerhetskrav vid systemanvändning (kravkategori Enskilt system)

3.1 Grundkrav från kravanalys (klassningsvärde 111)

Alla användare av systemet/systemen ska ha en unik användaridentitet, dvs. inga gruppidentiteter får finnas.

Defaultlösenord från leverantör måste bytas ut.

En kontinuitetsplan ska tydliggöra hantering i ett läge då systemet/tjänsten inte finns tillgänglig under en längre tid (läs katastrofläge)

3.2 Tillkommande krav då någon av aspekterna konfidentialitet eller riktighet når upp till ett klassningsvärde som överstiger 1

Tilldelning av sysadmin- och användarkonton med höga behörigheter ska begränsas samt granskas och revideras vart annat år. Dessa ska omfatta att medge, förändra och återkalla åtkomst till information, system och tjänster.

Vid access utanför det fasta nätet ska organisationens VPN-tjänster för säker internetuppkoppling användas.

Riskbedömning ska göras innan leverantörer eller andra externa parter ges tillgång till systemen/systemet.

All personal som hyrs in från leverantörer till systemet/systemen ska vara informerade om de säkerhets- och sekretesskrav som har avtalats.

Regelbundna uppföljnings- och planeringsmöten med leverantörer till systemet/systemen bör genomföras minst en gång per år.

Personuppgiftsincidenter, säkerhetsincidenter och säkerhetsbrister ska anmälas och följas upp enligt organisationens rutiner.

3.3 Tillkommande krav då någon av aspekterna konfidentialitet eller riktighet når upp till klassningsvärde 3

Åtkomsträttigheter via sysadmin- och användarkonton med höga behörigheter ska granskas minst en gång per år.