Råd för organisering av säkerhetsarbetet

eSams expertgrupp för säkerhet har tagit fram dessa råd för organisering av säkerhetsarbetet.

Det har efterfrågats enkla råd för hur säkerhetsarbetet bör organiseras, i synnerhet avseende informationssäkerhet, där regleringen inte är lika tydlig som för exempelvis säkerhetsskydd. Det är uppenbart att det finns stora skillnader mellan hur olika organisationer löst frågan och såväl myndighetsledningar som säkerhetsexperter har lyft frågan och det finns en osäkerhet kring vad som är ”rätt” utformning och omfattning. Såväl *MSBFS 2016:1*, *ISO 27000-serien* samt *Metodstöd för systematiskt informationssäkerhetsarbete* ger bra underlag för vad organisationen bör tänka. eSams expertgrupp för säkerhet vill särskilt peka på några grundläggande punkter som organisationens ledning bör ta hänsyn till:

1. Ytterst är det ledningen för organisationen som är ansvarig för säkerheten och dess uppföljning.

2. Ansvaret för säkerhet följer verksamhetsansvaret både strategiskt och operativt och på alla nivåer. Ansvaret och mandat ska beskrivas i styrande dokument, som arbetsordning eller motsvarande. Säkerhetsarbetet ska ingå i den ordinarie verksamheten och beskrivas i verksamhetsplaneringen med aktiviteter som följs upp.

3. Organisationen ska ha en centralt ansvarig funktion för ledning och samordning av det systematiska säkerhetsarbetet och som i en oberoende roll rapporterar till ledningen. Den specifika utformningen är beroende av organisationens uppdrag och vilka författningar som styr verksamheten.

4. Ledningen ska säkra att det, utifrån organisationens uppdrag, finns dokumenterade roller, ansvar, kompetens och resurser för säkerheten, exempelvis för områdena it-säkerhet, arkitektur, juridik, skydd för personuppgifter, utveckling och upphandling.

5. Organisationens funktioner och rutiner för riskhantering och uppföljning ska omfatta säkerhetsrisker, utformade utifrån organisationens uppdrag.

6. Ansvarsfördelningen ska vara klargjord i fall där ordinarie organisationsfunktioner kan uppleva oklarheter, exempelvis i samband med utvecklings- och förändringsarbete, utkontraktering eller uppdrag som är funktions- och organisationsöverskridande.

7. Extern samverkan ska vara etablerad för att säkra kompetensutveckling, omvärldsbevakning samt förmåga att hantera oförutsedda händelser.

Läs mer

- MSB:s föreskrift 2016:1 om informationssäkerhet: https://www.msb.se/sv/regler/gallande-regler/krisberedskap-och-informationssakerhet/msbfs-20161/
- Information från SIS om ISO 27000-serien: https://www.sis.se/iso27000/dettariso27000/
- Metodstödet på informationssäkerhet.se: https://www.informationssakerhet.se/metodstodet/utforma/
- För myndigheter som lyder under säkerhetskyddslagstiftningen finns mer information bland annat här: https://www.sakerhetspolisen.se/sakerhetsskydd.html
- Krav på organisation och ansvar kring dataskydd finns bland annat här: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/