HÖGSKOLAN
I HALMSTAD

Rutinbeskrivning: Granskning och uppföljning av informationssäkerheten

Fastställd av IT-chef 2018-10-10, dnr I 2018/64

Bakgrund

Detta dokument specificerar hur granskning, uppföljning, rapportering och utvärdering av Högskolans arbete med informationssäkerhet ska gå till. Såväl den konkreta informationssäkerheten, den tekniska miljön och rutinerna, som modell och metod för hur Högskolan arbetar med informationssäkerhet ska granskas och utvärderas.

Granskning och uppföljning

Enligt befintligt regelverk ska den information som hanteras inom Högskolans centrala och administrativa IT-system genomgå informationsklassning och den information där en förlust av informationens konfidentialitet, riktighet eller tillgänglighet kan få allvarliga eller betydande konsekvenser för Högskolans verksamhet eller enskilda individer dessutom genomgå riskbedömning med avseende på informationssäkerhet. Till detta kommer även regler kring hantering av information och rapportering och åtgärdande av informationssäkerhetsincidenter.

Rutiner för tilldelning och uppdatering av behörigheter i IT-system dokumenteras och uppdateras årligen genom Högskolans systemförvaltningsmodell.

Informationssäkerhetsansvarig ska årligen granska dokumentationen ovan, med fokus på följande punkter:

- Finns uppdaterad informationsklassning för den information som hanteras vid Högskolan?
- Är riskbedömning gjord för den information som regelverket kräver?
- Har riskbedömning gjorts för information som hanteras i nya IT-system, och för information i IT-system som bytt driftform under året?
- Planeras riskbedömning för informationen i de IT-system som kommer att bytas ut eller upphandlas under det kommande året?
- Har planerade åtgärder, som har sin grund i riskbedömning, genomförts?
- Uppfyller förvaltningsobjektens rutiner kring behörighetstilldelning Högskolans regelverk? Dokumenteras behörighetstilldelningen enligt Högskolans regelverk?

Rapportering

En gång per år ska styrelsen få en rapport om läget kring informationssäkerheten vid Högskolan. Där ska framgå dels genomförda aktiviteter och inträffade incidenter under senaste året samt hur man arbetat för att minska risken för upprepning av incidenterna, dels en beskrivning av aktiviteter som kan behöva utföras under kommande år för att informationssäkerheten vid Högskolan ska ligga kvar på samma, eller högre, nivå som tidigare. Rapporten ska innehålla följande:

- Resultatet från informationssäkerhetsansvarigs granskning i punkten ovan,
- Resultat från eventuella externa granskningar
- Genomförda aktiviteter i enlighet med regelverket
- Eventuell informationssäkerhetshöjande aktiviteter som genomförts (t.ex. genomförda utbildningar, tekniska åtgärder, förbättrade rutiner)

- Information om och analys av inträffade incidenter
- Uppföljning av aktiviteter med grund i tidigare rapporter till styrelsen
- Krav från och händelser i omvärlden som påverkar Högskolans informationssäkerhet

En gång per år (eller oftare, vid behov) ska systemägarna få motsvarande rapport.