HÖGSKOLAN
I HALMSTAD

Rutinbeskrivning: Riskbedömning med avseende på informationssäkerhet

Fastställd av IT-chef 2018-10-10, dnr I 2018/60

Innehållsförteckning

Bakgrund

Genom att arbeta med riskbedömningar med avseende på informationssäkerhet får Högskolan en viktig grund för att kunna utforma ett väl anpassat, säkert och kostnadseffektivt skydd för sin information.

Att identifiera och kartlägga risker som utgör hot mot verksamheten är den första fasen i riskhanteringsarbetet. Såväl risker som har förverkligats i form av skadehändelser och tillbud som risker som kan drabba verksamheten i framtiden ska listas. Det är viktigt att ta del av olika medarbetares kunskap inom respektive område. Normalt deltar alltid systemförvaltare, och minst en av systemägare, objektägare och verksamhetsansvarig i riskbedömningen. Andra personer, med kunskap inom området, kan delta vid behov.

Både verksamhetskrav och omvärldskrav ska användas vid bedömningen av hotbild, risker och sårbarheter i samband med användning av teknik för informationsbehandling och datakommunikation.

Det primära resultatet av en riskbedömning är en förteckning av risker, deras potentiella skadeverkan och tänkbara sätt att hantera riskerna.

Riskbedömningens innehåll

1: Välj och beskriv bedömningsobjekt

Normalt görs riskbedömningen på de informationstillgångar där informationsklassningen resulterat i konsekvensen Allvarlig eller Betydande för något av kriterierna Konfidentialitet, Riktighet eller Tillgänglighet. Riskbedömning görs också inför byte av IT-system, och inför byte av driftform för IT-system.

- Gå igenom och komplettera beskrivningen från informationsklassningen av de informationstillgångar som ska bedömas.
- Dokumentera eventuella avgränsningar.

2: Identifiera riskerna

- Vilka är riskerna för de valda informationstillgångarna? Vad kan inträffa?
- Varje risk ska vara tydligt beskriven och satt i sitt sammanhang. Utan att specificera är det svårt att gå vidare med riskbedömning kring, och åtgärder mot, en risk. Det är viktigt att alla förstår och är överens om innebörden i riskerna.

Vissa risker kan rikta sig mot flera informationstillgångar, inom eller utom den pågående riskbedömningen; notera om de behöver hanteras i samband med fler/andra förvaltningsobjekt.

3: Bedöm konsekvens och sannolikhet

- Bedöm vilka konsekvenserna blir om risken inträffar

  Konsekvensen är ett mått på den skada ett hot skulle ha på verksamheten om det inträffade. Skadan kan exempelvis vara direkt eller indirekt, ekonomisk eller medmänsklig. Följande nivåer används:

Försumbar: mycket små konsekvenser för enstaka personer, små ekonomiska eller andra konsekvenser för Högskolan.

Måttlig: negativa konsekvenser för enstaka personer, ekonomiska eller andra tillgångar för Högskolan

Allvarlig: risk för skada på personer, risk för betydande ekonomiska eller andra konsekvenser för Högskolan.

Katastrofal: verklig fara för personer, stora ekonomiska eller andra konsekvenser för Högskolan.

- Bedöm sannolikheten för att hotet ska inträffa

  Sannolikheten anger hur troligt det är att hotet kommer att inträffa[1]:

  Mycket sällan: en gång på en tioårsperiod

  Sällan: en gång på en femårsperiod

  Regelbundet: 1-5 gånger per år

  Ofta: mer än 5 gånger per år

Definitionerna av konsekvens och sannolikhet kan förändras. Eventuella förändringar ska dokumenteras.

- Sätt in varje enskild risk på sin plats i en konsekvens- och sannolikhetsmatris (se nedan). Med matrisens hjälp bedöms sedan risken för att något inträffar.

[1] I tidigare versioner av rutinen användes andra frekvenser för sannolikhet. Det innebär att sannolikheter inte är helt jämförbara under en tvåårsperiod.

5: Ta fram åtgärdsförslag

- Gå igenom de identifierade riskerna och ta fram förslag på hur dessa ska hanteras. Risker med stor sannolikhet och stor konsekvens bör ofta åtgärdas så snabbt som möjligt.
- Diskutera, med utgångspunkt i matrisen, eventuella åtgärdsförslag och prioritetsordningen mellan dessa
- Ta fram en rekommendation med förslag på åtgärder och förbättringar för att eliminera, reducera eller acceptera riskerna
- Diskutera behovet av sekretess för riskbedömningen – den är troligtvis känslig.

Sammanställning och rapport

Resultatet ska sammanställas. Det är viktigt att all tänkbar information, eventuella avsteg eller nya definitioner, inkluderas i slutresultatet.

Sammanställningen ska innehålla eventuella förslag till åtgärder och rekommendationer till den som ska fatta beslut. Ev åtgärder hanteras inom ramen för systemförvaltningsmodellen.