HÖGSKOLAN
I HALMSTAD

Rutinbeskrivning: Informationsklassning

Fastställd av IT-chef 2018-10-10, dnr I 2018/59

Innehållsförteckning

Bakgrund

Att Högskolan i Halmstad definierat sina informationstillgångar och klassificerat dem i förhållande till skyddsbehovet är en av grunderna till att kunna ha en effektiv informationssäkerhet. Informationsklassningen ser dels till informationens typ, och dels till de konsekvenser det skulle medföra om informationen förvanskades, försvann, kom obehörig till del osv.

Utförande

Informationstillgångarna klassificeras utifrån de konsekvenser som oönskad påverkan kan leda till. Om till exempel Högskolan lider allvarlig skada av att en informationstillgång som är viktig för verksamheten ändras på ett felaktigt sätt, ska denna information placeras i en klass med hög konsekvensnivå avseende riktighet.

Informationsklassningen sker genom att verksamheten i tur och ordning

1. beskriver de informationstillgångar som omfattas (till exempel studieresultat, eller ekonomiska uppgifter) och specificerar om de omfattar personuppgifter eller känsliga personuppgifter (enligt dataskyddsförordningens definition),
2. definierar informationen som Öppen, Intern, Skyddsvärd eller Särskilt skyddsvärd. Vid definitionen ser man till flera kriterier, Till exempel ekonomiskt värde, legala krav, känslighet och betydelse för Högskolans verksamhet eller enstaka individer, och
3. per säkerhetsaspekt, placerar in informationstillgångarna i de olika konsekvensnivåerna.

Varje informationstillgång ska klassificeras i en av konsekvensnivåerna för varje säkerhetsaspekt (konfidentialitet, riktighet, tillgänglighet). Notera att varje säkerhetsaspekt ska klassificeras separat; varje informationstillgång kan ges olika konsekvensnivå för respektive aspekt. Ett speciellt malldokument finns framtaget för detta.

Särskild hänsyn ska tas till möjligheter och risker vid kombination av information (i synnerhet när det gäller konfidentialiteten).

Utifrån klassificeringen ovan gäller olika krav för hantering av informationen, till exempel hur informationen ska vara nåbar, eller var den får lagras. Dessa krav gäller även för information utanför de centrala IT-systemen.

Säkerhetsaspekter

Klassificeringen ska göras för tre aspekter av informationssäkerhet: konfidentialitet, riktighet och tillgänglighet. Det finns i Sverige flera allmänt vedertagna definitioner av dessa aspekter. Högskolan i Halmstad har valt dessa definitioner:

Konfidentialitet: Kallas ibland sekretess. Innebär att ingen obehörig ska ha åtkomst till informationen. Konsekvensnivån för konfidentialiteten har endast att göra med informationens skyddsbehov. Konfidentialiteten har ingen koppling till sekretesslagen – sekretessprövning ska alltid göras i varje enskilt fall av utlämnande av information.

Riktighet: Innebär att information inte oavsiktligt förändras, vare sig obehörigen, av misstag, eller på grund av funktionsstörning.

Tillgänglighet: Innebär att informationstillgångar är åtkomliga på förväntat sätt och inom önskad tid. Förlust av tillgänglighet kan graderas, till exempel kan förlusten uppstå genom fördröjning (där tidsgränser för allvarlig, betydande etc. är beroende av sammanhanget) eller genom att information förstörts.

Värderingen kan också göras ur andra aspekter.

Konsekvensnivåer

När informationen definierats ska den relateras till den konsekvens som uppkommer när informationen är felaktig, inte är tillgänglig, eller sprids på ett otillåtet sätt. Varje säkerhetsaspekt klassificeras i en av tre konsekvensnivåer: Måttlig, Betydande respektive Allvarlig konsekvens. Dessa konsekvensnivåer påverkar de krav som ställs på skyddet av informationen.

Måttliga konsekvenser

Förlust av konfidentialitet, riktighet eller tillgänglighet hos information som innebär måttlig negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller på enskild individ. Till exempel en brist som för Högskolan eller annan verksamhet kan medföra obehag eller begränsad ekonomisk förlust för enskilda personer, eller begränsad skada för Högskolan eller tredje part. Ett systemavbrott ska normalt inte vara längre än fyra timmar, men kan vara upp till ett par veckor vid mycket allvarliga händelser.

Betydande konsekvenser

Förlust av konfidentialitet, riktighet eller tillgänglighet hos information som innebär betydande negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller på enskild individ. Till exempel en brist som för Högskolan eller annan verksamhet kan orsaka omfattande obehag eller ekonomisk förlust för enskilda personer, eller omfattande skada för Högskolan eller tredje part. Ett systemavbrott ska normalt inte vara längre än en timme, men kan vara upp till ett dygn vid mycket allvarliga händelser.

Allvarliga konsekvenser

Förlust av konfidentialitet, riktighet eller tillgänglighet hos information som innebär allvarlig eller katastrofal negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller på enskild individ. Till exempel en brist som för Högskolan eller annan verksamhet kan medföra skada på liv eller hälsa för enskilda personer, orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer, eller mycket allvarlig skada för Högskolan eller tredje part. Ett systemavbrott ska normalt inte vara längre än några minuter, ens vid mycket allvarliga händelser.

Exempel på informationstyper

Öppen information

Till exempel sådant som publiceras på hh.se.

Här ställs inga specifika krav kring konfidentialitet.

Intern information

Till exempel sådant som publiceras på Insidan.

Här är det viktigt att se till att inte icke-anställda, till exempel konsulter/leverantörer, inte har möjlighet att läsa informationen.

Skyddsvärd information

Till exempel underlag till kommande allmänna handlingar.

Här är det dessutom viktigt att se till att informationen inte går förlorad. Därför bör informationen lagras inom Högskolans nätverk.

Särskilt skyddsvärd information

Till exempel material inom pågående upphandlingar.

Här är det dessutom viktigt att se till att behörigheter till exempelvis delade mappar och i IT-system är korrekt satta, och att utskrifter inte glöms i skrivare.

Personuppgifter

Till exempel klasslistor eller anmälningslistor.

De personuppgifter som Högskolan ansvarar för får endast lagras inom Högskolans nätverk, eller hos de leverantörer som Högskolan skrivit personuppgiftsbiträdesavtal med. Personuppgifter får inte sparas längre tid än nödvändigt eller användas till annat syfte än vad som ursprungligen var tänkt. Personuppgiftsbehandlingar ska anmälas till Högskolans arbetsgrupp för dataskydd, enligt specifik rutin.

Känsliga personuppgifter

Till exempel journalanteckningar och sjukintyg