Modell

2020-10-26

DNR: MIUN 2020/2488

Modell för klassificering av information

Publicerad: 2020-11-05

Beslutsfattare: Helena Wallskog

Handläggare: Eva Rodin Svantesson

Beslutsdatum: 2020-11-05

Giltighetstid: Tillsvidare

Ansvarig för förvaltning: Modellen förvaltas av infrastrukturavdelningen.

Målgrupp: Infrastrukturavdelningen (INFRA).

Sammanfattning: Modellen beskriver hur arbetet med klassning av information ska genomföras på Mittuniversitetet. Modellen har anpassats utifrån Myndigheten för samhällsskydd och beredskaps föreskrifter MSBFS 2020:6-7.

Innehållsförteckning

1. Modell för klassificering av information

1.1 Allmänt

Informationsklassificering ingår som en del i det systematiska informationssäkerhetsarbetet. Klassningen görs utifrån flera kriterier. De kriterier som tas upp i LIS (dvs SS-ISO/IEC 2700-serien) är rättsliga krav, värde, verksamhetsbetydelse och känslighet för obehörigt röjande eller modifiering.

Enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) ska Myndigheten enligt 6§ säkerställa att informationssäkerhetsarbetet är systematiskt och riskbaserat genom att
1. klassa sin information avseende konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få (informationsklassning),
2. identifiera, analysera och värdera risker för sin information (riskbedömning),
3. utifrån genomförd informationsklassning och riskbedömning identifiera behov av och införa ändamålsenliga och proportionella säkerhetsåtgärder, och
4. utvärdera säkerhetsåtgärderna och vid behov anpassa skyddet av informationen. I arbetet ingår att genomföra en gapanalys.

Informationssäkerhetsarbetet och införda säkerhetsåtgärder ska dokumenteras.

Mittuniversitets modell beskriver hur arbetet med informationsklassificeringen ska genomföras. Som stöd i arbetet finns:

- modellen för informationsklassning,
- klassningsstöd med exempel,
- mallen där klassningen ska dokumenteras
- mall för omvärldsanalys
- mall för rättliga krav
- riskvärdering och riskmatris
- skyddsåtgärder.

Genomförd klassning av respektive informationstillgång ska diarieföras med sekretessmarkering.

Redovisning av att ett verksamhetssystem har klassat sin information dokumenteras i det aktuella systemets förvaltningsplan. Systemgruppsägaren ansvarar för att klassningen genomförs.

Ägare av informationstillgångar är respektive chef vilken också ansvarar för informationsklassningen.

1.2 Användningsområden

Konkreta användningsområden där en informationsklassificering bör ligga till grund för val av säkerhetsnivå och därav följande säkerhetsåtgärder är:

- Fastställande av skyddsnivå för forskningsdata.
- Kravställning/kravspecificering inför systemutveckling eller upphandling av system (se MSB:s vägledning - informationssäkerhet i upphandling).
- Fastställande av säkerhetsdesign av ett informationssystem.
- Genomförande av risk- och sårbarhetsanalyser av ett systemförvaltningsobjekt eller ett enskilt informationssystem.
- Genomförande av säkerhetsanalyser (egenkontroller) i ett förvaltningsobjekt eller enskilt informationssystem.

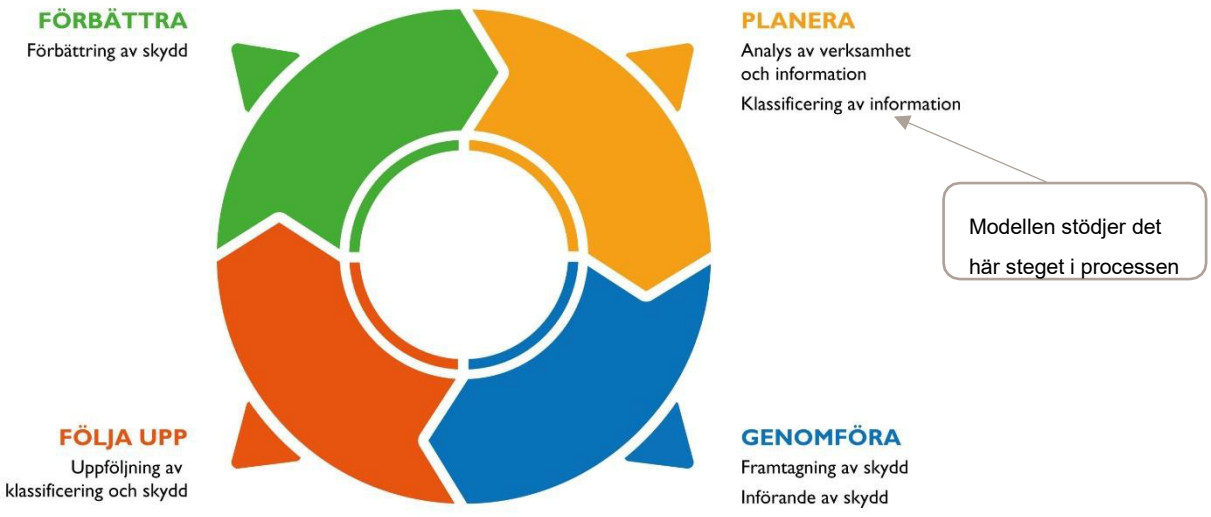
1.3 Riskbedömning

Verksamheten ska i samband med informationsklassningen beskriva vilka risker som har identifierats i samband med att informationen hanteras i en digital miljö.

Alla de risker som kan vara utifrån utformningen av organisationen, processer och förfaranden, rutiner för förvaltning, beroendet av medarbetare, den fysiska miljön, hur konfiguration av informationssystem utförs, användningen av maskin-, programvaru- eller kommunikationsutrustning och beroendet av externa parter ska beaktas.

Riskerna ska hanteras på ett lämpligt sätt t.ex genom att identifiera vilka säkerhetsnivåer som behöver vidtas för att få rätt skyddsnivå. Genomförda riskbedömningar ska dokumenteras och diarieföras tillsammans med informationsklassningen

1.4 Klassificering av information i informationssäkerhetsprocessen



1.4.1 Klassificering av information

Klassificering av information är en grundläggande aktivitet för att information och resurser ges nödvändigt skydd. Det är informationen som är skyddsobjektet, d v s det som ska skyddas. Informationen ska klassificeras utifrån den funktion och betydelse för verksamheten som den har och de konsekvenser det medför om informationen skulle hanteras felaktigt, försvinna, komma i orätta händer etc. alltså till följd av otillräcklig konfidentialitet, riktighet och tillgänglighet:

Aspekt	Konsekvens
Konfidentialitet:	Att informationen skyddas från obehörig insyn
Riktighet:	Att informationen inte ändras på ett obehörigt sätt
Tillgänglighet:	Att informationen finns tillgänglig för rätt person vid rätt tillfälle

1.4.2 Konsekvensnivåer

I modellen klassificeras information utifrån de konsekvenser som oönskad påverkan på informationens kvalitet bedöms leda till. Konsekvenserna värderas i termer av oönskad påverkan på verksamheten eller annan part till följd av otillräcklig konfidentialitet, riktighet eller tillgänglighet.

I modellen används fyra nivåer för värdering av konsekvenser. För de system som klassificeras i klass 2 och 3 vad gäller konfidentialitet, riktighet eller tillgänglighet ska en riskanalys genomföras.

Nivå	Definition
Informationsklass 0 (försumbar)	Inga konsekvenser
Informationsklass 1 (låg, måttlig)	Kan medföra obehag eller begränsad ekonomisk förlust för enskilda personer, eller begränsad skada för universitetet eller tredje part
Informationsklass 2 (medel, betydande)	Kan orsaka omfattande obehag eller ekonomisk förlust för enskilda personer, eller omfattande skada för universitet eller tredje part
Informationsklass 3 (hög, allvarlig)	Kan medföra skada på liv eller hälsa för enskilda personer, eller orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer, eller mycket allvarlig skada för universitetet eller tredje part

1.4.2.1 Konfidentialitet

Informationen ska vid informationsklassning bedömas utifrån kravet på konfidentialitet. Konfidentialitet innebär att informationen inte får tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer. Kravet på konfidentialitet klassificeras mot de klasser som återfinns i dokumentet ”Klassningsstöd med exempel på konsekvensnivåer”.

1.4.2.2 Riktighet

Informationen ska vid informationsklassning bedömas utifrån kravet på riktighet. Riktighet innebär att informationen ska vara korrekt och fullständig. Kravet på riktighet klassificeras mot de klasser som återfinns i dokumentet ”Klassningsstöd med exempel på konsekvensnivåer”.

1.4.2.3 Tillgänglighet

Informationen ska vid informationsklassning bedömas utifrån kravet på tillgänglighet. Tillgänglighet innebär att informationen ska vara åtkomlig och användbar på begäran från ett behörigt objekt. Kravet på tillgänglighet klassificeras mot de klasser som återfinns i dokumentet ”Klassningsstöd med exempel på konsekvensnivåer”.

1.5 Sammanfattning

Resultatet från de tre olika klassificeringarna skall utgöra det samlade kravet på nivån för skyddet av den aktuella informationen eller verksamhetssystemet.