REKTORS KANSLI

2023-03-13 Dnr C2023/270

Riktlinjer för riskhantering i ledningssystem för informationssäkerhet (LIS) vid Karlstads universitet

Syfte

Riktlinjernas syfte är att beskriva hur risker som kan påverka Karlstads universitets informationssäkerhet ska identifieras, analyseras och hanteras. Riktlinjerna är framtagna för att stödja verksamheten att uppfylla kraven i MSB:s föreskrift om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

MSB:s metodstöd för informationssäkerhet samt Riktlinjer för informationssäkerhet i Västra Götalandsregionen har använts som mall och inspiration.

Riktlinjerna är ett av de underdokument som kompletterar styrdokumentet Informationssäkerhetspolicy vid Karlstads universitet.

Det huvudsakliga arbetet med att ta fram riktlinjerna har utförts av Informationshanteringsrådet i samråd med IT-chefen och säkerhetschefen.

Beslut:	RB 45/23	Dnr:	C2023/270	Ersätter:	-	Dnr:	-
Giltighet fr.o.m:	2023-03-13	t.o.m:	Tills vidare	Handläggare:	Niklas Nikitin		

1 Inledning

Det är viktigt att Karlstads universitet känner till, bedömer och hanterar de risker som kan inverka på myndighetens informationshantering. Risker ska därför identifieras och analyseras, och riskägare ska ta ställning till hur riskerna ska hanteras.

2 Omfattning

Riktlinjen gäller för all hantering av Karlstads universitets informationstillgångar oavsett var eller i vilken form hanteringen sker.

3 Definitioner

Definitionerna nedan kommer från SIS-TR 50:2015[1] eller SS-ISO/IEC 27000:2020 om inte annat uttryckligen anges.

Analysobjekt: det som ska analyseras. Kan ha olika omfattning beroende på analysens syfte och deltagarnas kompetenser[2].

Informationshantering (inom ramen för LIS vid Karlstads universitet): insamling, behandling, lagring och överföring av information så att informationen kan användas på ett ändamålsenligt och kontrollerat sätt.

Informationstillgång: all information som är av värde för en organisation.

Konsekvens: resultat av en händelse med negativ inverkan.

Sannolikhet: ett mått på hur troligt det är att ett hot realiseras.

Säkerhetsåtgärder: identifierad uppsättning åtgärder för att möta en organisations risker.

Risk: produkten av konsekvens och sannolikhet för att ett hot realiseras.

Riskägare: funktion som ansvarar för och har befogenhet för att hantera en risk.

4 Riskhantering

Riskhantering är samordnade aktiviteter för att leda och styra en organisation med avseende på risk. Riskhantering inom LIS hos Karlstads universitet, se Figur 1, ska tillämpas av varje verksamhet (exempelvis fakultet, institution eller avdelning) och vara en del av beslutsunderlaget inför förändringar. Riskhantering inom LIS ska ske i enlighet med Karlstads universitets metodstöd för riskhantering. Ansvaret för att ta fram och regelbundet uppdatera ett metodstöd för riskhantering inom LIS ligger hos Informationshanteringsrådet på Karlstads universitet.

Riskhantering inom LIS avseende verksamhetens informationshantering ska genomföras regelbundet. Periodiciteten beslutas utifrån verksamhetens behov.

De olika stegen i riskhanteringsprocessen ska alltid genomföras:

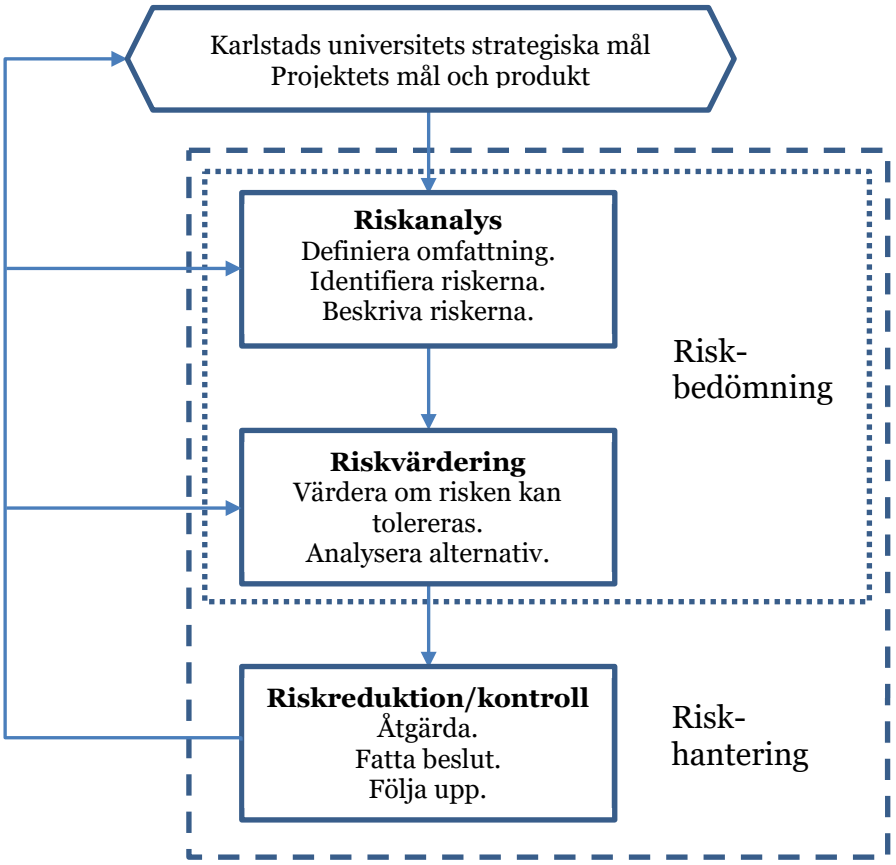
- Vid större förändring i verksamhetens informationshantering

---

[1] Termer, definitioner och förklaringar är återgivna ur SIS Tekniska rapport, Terminologi för informationssäkerhet, utgåva 1, med vederbörligt tillstånd från SIS Förlag AB.

[2] Definierat i MSB metodstöd för informationssäkerhet, https://www.informationssakerhet.se

- Vid upphandling av nya informationssystem
- Vid förändrad användning av ett informationssystem, exempelvis:
    - Större förändringar av systemförvaltning
    - Förändrad användning av informationssystemet eller informationssystemets säkerhetsåtgärder
    - Höjd risk på grund av förändrad personuppgiftshantering
    - Förändrad omvärld som påverkar informationshanteringen
- I andra situationer då det kan förväntas att riskerna ökar



Figur 1 Schematisk bild av riskhanteringsprocessen

4.1 Riskbedömning

En viktig del i riskhanteringsprocessen är riskbedömningen. Den ska vara en del av beslutsunderlaget inför förändringar och ska göras i ett förebyggande syfte. Riskbedömningen leder till att ett lämpligt val av säkerhetsåtgärder genomförs i syfte att minska myndighetens risknivå.

En riskbedömning kan kort beskrivas som svaret på tre frågor:

- Vad kan hända?
- Hur sannolikt är det?
- Vad blir konsekvensen om det händer?

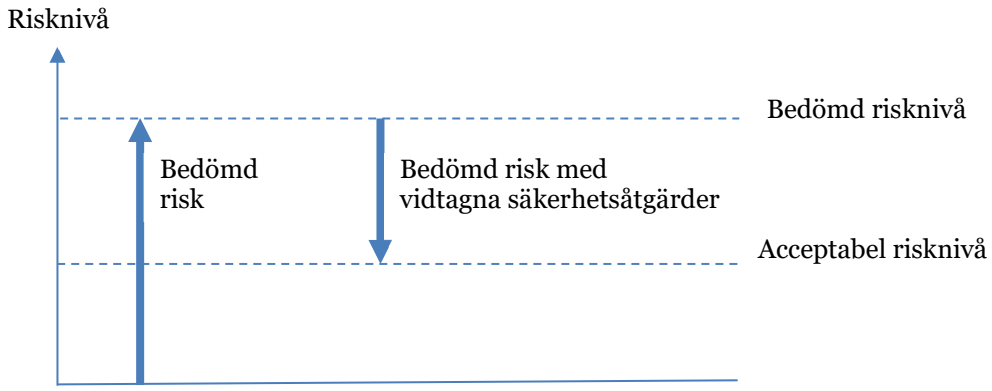
En hörnsten i utformningen av Karlstads universitets riskhanteringsprocess är att fastställa utifrån vilka kriterier risker ska värderas. Det är viktigt att risker värderas på ett så likartat sätt som möjligt i hela myndigheten eftersom risker är underlag för beslut och prioritering. Obefintliga eller otydliga kriterier kan få följden att likvärdiga risker värderas olika och därmed prioriteras olika eller till och med att låga risker värderas högre än allvarliga risker. Detta kan få till följd att myndigheten gör felaktiga prioriteringar, och därmed inför otillräckliga säkerhetsåtgärder eller lägger resurser på onödigt kostsamma säkerhetsåtgärder.

Som stöd till riskbedömningen ska Karlstads universitets Riktlinjer för normskala som huvudregel användas.

4.2 Riskreduktion/kontroll

För att nå syftet med själva riskhanteringen, nämligen att informationen ska ha adekvat skydd, behöver informationen skyddas av säkerhetsåtgärder. Val av säkerhetsåtgärder ska ske på ett systematiskt sätt.

I bland annat den internationella standarden för informationssäkerhet (ISO/IEC 27002) samt Riksarkivets och MSB:s föreskrifter finns ett antal säkerhetsåtgärder beskrivna. Vissa av dem kan ses om en del av styrningen av informationssäkerhetsarbetet medan andra är konkreta åtgärder för att ge skydd i hantering av information. Olika säkerhetsåtgärder behöver ofta kombineras för att ge tillräckligt skydd. Målet är att riskerna efter vidtagna säkerhetsåtgärder ska ligga på en acceptabel nivå, se Figur 2.



Figur 2, Relation mellan bedömd risk och säkerhetsåtgärder

För att kontrollera om effekten är den önskade ska genomförda aktiviteter och fattade beslut dokumenteras. Riskägaren ansvarar för uppföljning av säkerhetsåtgärdernas resultat.

5 Ansvar

Informationsägare[3], systemägare[3] och teknikresursägare[3] är ansvariga för att initiera riskhantering för sina respektive ansvarsområden och dess omfattning.

Universitetsdirektören är ansvarig för att initiera riskhanteringen inom LIS som gäller övergripande informationssäkerhetsrisker för Karlstads universitet som helhet.

[3] Se Riktlinjer för ansvar och roller i LIS.

Kvarvarande hot och risker som kan innebära allvarliga konsekvenser för Karlstads universitet ska eskaleras uppåt i organisationen, i enlighet med Riktlinjer för ansvar och roller i LIS.

6 Stöd

Informationssäkerhetsanvarig är ett stöd till verksamheten vid genomförandet av riskhantering i LIS.