

Informationssäkerhet

Stöd- och vägledning riskhantering

Östhammars kommun

Målgrupp	Chefer och nyckelpersoner, alla kontor och verksamheter
Avsändare	Kommunledningskontoret, Digitalisering och projektledning
Dokumentansvarig	Informationssäkerhetssamordnare
Framtagen	2024-10-10
Aktualitetsprövad	2026-03-05

Innehåll

Innehåll.....	3
Mål och syfte	3
Riskhantering	3
Riskanalys	3
Dokumentation	3
Genomförande	3
Mallar för dokumentation.....	5

Innehåll

Innehållet utgår från kommunens program och vägledning för informationssäkerhet och ger en fördjupad beskrivning över **riskhantering** och förklarar arbetsprocessen med att skydda den information, inklusive personuppgifter, som kommunens verksamheter hanterar.

Mål och syfte

Målet är en ensad process för riskhantering som svarar mot externa krav, interna behov och som bidrar till att skydda informationen i kommunens verksamheter.

Syftet är att säkra kvalitén i kommunens arbete med informationssäkerhet genom att identifiera omständigheter som utgör en väsentlig risk och kräver åtgärd och uppföljning. Arbetet omfattar även de IT-tjänster som används för kommunens informationshantering.

Riskhantering

Efter genomgångna skyddsåtgärder dokumenteras och hanteras nu eventuellt kvarstående risker. Det utförs genom att analysera, bedöma, hantera och följa upp risker.

Hanteringen kan bestå av att sätta in åtgärder som minskar eller eliminerar sannolikheten att det inträffar och/eller konsekvensen av att det inträffar. Riskägare och ev. riskhanterare ska dokumenteras.

Acceptans av risker med högt riskvärde, allvarliga skadekonsekvenser och kostsamma skyddsåtgärder bör beslutas av ansvarig nämnd eller kommunstyrelsen (om flera verksamheter berörs) och en riskacceptans¹ ska dokumenteras.

Riskanalys

Riskanalys avser sannolika händelser med konsekvens för KRT (konfidentialitet, riktighet, tillgänglighet). Riskerna bör vara rimliga, inte teoretiska risker som har en väldigt låg sannolikhet att det händer. Fokusera på det man kan göra någonting åt!

Dokumentation

Riskanalysen ska dokumenteras och aktuella versioner finnas tillgängliga i respektive verksamhet. I kommunens verktyg dokumenterar informationssäkerhetsteamet aktuella informationstillgångar (som t.ex. system och applikationer) med tillhörande riskanalyser. Om inte riskanalysen är gjord tillsammans med informationssäkerhetsteamet -och därmed redan dokumenterad i verktyget - är det viktigt att komma ihåg att skicka en kopia på riskanalysen till infosakerhet@osthammar.se. Om analysen innehåller känsliga uppgifter, kolla med informationssäkerhetsteamet vilken säker kanal som kan användas.

Genomförande

1. **Identifiering av risker, hot och sårbarheter** – Ange de risker, hot och sårbarheter som finns och beskriv dessa.
2. **Riskbedömning - värdera riskerna** – Hur stor är sannolikheten att det händer? Vad blir konsekvensen om det händer?

¹ Att acceptera en risk. T.ex. saknas sätt att hantera risken eller så är kostnaden för åtgärder större än eventuell konsekvens kostnader.

Genom att värdera riskerna får man fram **riskvärdet** (= konsekvens x sannolikhet)

Mycket hög		Sannolikhet	Konsekvens
Hög	4	Inträffar flera gånger per år	Allvarlig
Medelhög	3	Inträffar en gång per år	Betydande
Låg	2	Inträffar sällan, en gång på 5-10 år	Måttlig
	1	Inträffar < 10-20 år	Försumbar

Konsekvens	Allvarlig	4	8	12	16
	Betydande	3	6	9	12
	Måttlig	2	4	6	8
	Försumbar	1	2	3	4
Riskvärde= konsekvens*sannolikhet 1-2: Inga åtgärder behöver vidtas 3-6: Risker som behöver analyseras djupare. Behov av åtgärder ska utvärderas 8-12: Åtgärder måste vidtas 16: Åtgärder måste omedelbart vidtas		Osannolikt	Liten sannolikhet	Stor sannolikhet	Mycket stor sannolikhet
		Det finns mycket få eller inga tecken på att hotet är verklighet i dag	Inträffar sannolikt inte under normala omständigheter och i varje fall inte frekvent. Det finns vissa tecken på att hotet är verklighet i mindre omfattning i dag	Kan mycket väl inträffa men troligtvis inte särskilt frekvent. Det finns tydliga tecken på att hotet är verklighet i vissa delar av verksamheten och samhället redan idag	Sannolikheten är stor att det ska inträffa. Det är bekräftat att hotet är verklighet i väsentliga delar av verksamheten och samhället redan idag eller att den väntas bli det i närtid.
		Sannolikhet			

3. Riskhantering – beroende på riskvärde ta fram åtgärder – Ange och beskriv åtgärd, namn på riskägare, slutdatum och påverkan på riskvärde

Konsekvenskategorier att uppmärksamma:

ekonomisk förlust (större påverkan på verksamhetens budget)

verksamhetsavbrott

överträdelse eller bristande lagefterlevnad

personskada

skada för miljö - och hälsa, inklusive arbetsmiljö

skada på annan organisation eller samhället i stort

negativ påverkan på kommunen (dåligt varumärke, minskat förtroende)

Mall för dokumentation

Mall för riskhantering nås via INES [Arbeta med risker](#) och [Vägledning och stöd](#)