Regiondirektören

BESLUT

Alf Jönsson
Tfn: +46 44 309 31 21
Mail: alf.jonsson@skane.se

Datum: 2018-10-15
Dnr: 1800025

Instruktion för riskhantering avseende informations-tillgångar

Syftet med riskhantering är att analysera hot, risker och sårbarheter som kan påverka verksamheten och utifrån detta vidta lämpliga organisatoriska och tekniska säkerhetsåtgärder.

Instruktionen fastställer också vilka skalor och metoder som ska användas.

Härmed beslutas att:

- Instruktion för riskhantering avseende informationstillgångar fast-ställs
- Informationssäkerhetschef har uppdraget att underhålla instruktionen och genomföra ändringar som endast innebär liten påverkan samt har uppdrag att löpande underhålla tillhörande anvisning ”Riskhantering informationstillgångar”.

Alf Jönsson
Regiondirektör

Koncernkontoret
Enheten för säkerhet och intern miljöledning

Johan Reuterhäll
Informationssäkerhetschef
johan.reuterhall@skane.se

INSTRUKTION

Datum: 2018-08-27
Dnr:

Riskhantering avseende informationstillgångar

I takt med att omvärlden och den interna verksamheten förändras så förändras även behovet av skyddsåtgärder. Region Skåne behöver därför ha god kunskap om de hot, risker och sårbarheter som påverkar oss eller som kan komma att påverka oss. Detta åstadkoms genom omvärldsanalys och genom systematiskt arbete med riskbedömningar.

Region Skånes arbete med riskbedömningar regleras bland annat i

- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Dataskyddsförordningen (GDPR)
- Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap
- Myndigheten för samhällsskydd och beredskaps föreskrifter om landstings risk- och sårbarhetsanalyser (MSBFS 2015:4)
- Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)
- Säkerhetsskyddsförordningen (1996:633)

1 Bakgrund

I takt med att omvärlden och den interna verksamheten förändras så förändras även behovet av skyddsåtgärder. Region Skåne behöver därför ha god kunskap om de hot, risker och sårbarheter som påverkar oss eller som kan komma att påverka oss. Detta åstadkoms genom omvärldsanalys och genom systematiskt arbete med riskbedömningar.
Instruktionen ska användas för att genomföra den riskbedömning och riskbehandling som Regionstyrelsen beslutat om enligt ”Riktlinjer för informationssäkerhet”.

2 Syfte

Syftet med riskhantering är att analysera hot, risker och sårbarheter som kan påverka verksamheten och utifrån detta vidta lämpliga organisatoriska och tekniska säkerhetsåtgärder för att minska riskerna till en för verksamheten acceptabel nivå.

Instruktionen fastställer vilka skalor och metoder som ska användas vid bedömning och hantering av risker. För det praktiska genomförandet finns en anvisning som ska följas.

3 Mål

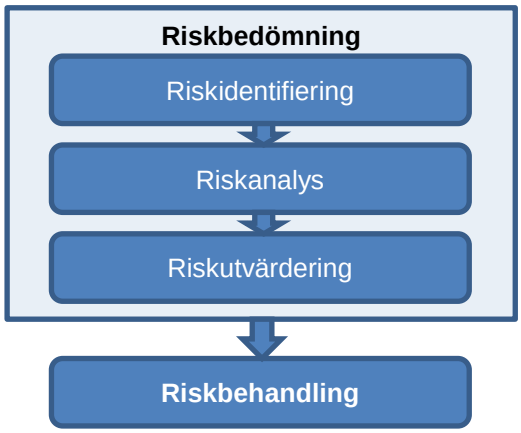
Målet är att risker identifieras och åtgärdas så att de blir acceptabla för Region Skåne.

4 Omfattning

Denna instruktion omfattar riskhantering avseende informationstillgångar. Exempel på informationstillgångar är:

- information
- program (applikationer, operativsystem samt mjukvara i medicintekniska produkter)
- tjänster (kommunikationstjänster, abonnemang etc.)
- fysiska tillgångar (datorer, medicintekniska produkter, datamedier, lokala nätverk etc.)
- personal
- immateriella tillgångar

Riskhanteringsprocessen omfattar riskbedömning och riskbehandling. I riskbedömningen ingår tre steg, riskidentifiering, riskanalys och riskutvärdering. Nedan figur illustrerar detta.



Figur 1 - Riskhanteringsprocessen

5 Målgrupp

- Informationsägare
- Linjechefer
- Informationssäkerhetssamordnare
- Verksamhetsansvariga och systemansvariga[1]
- Inköpare
- Projektledare

6 Ansvar

Informationsägaren ansvarar för att riskhantering genomförs och att informationshanteringen uppfyller interna och externa krav.

7 Genomförande

Riskhantering ska vara integrerat i Region Skånes arbetssätt och vara en kontinuerlig process som stödjer informationssäkerhetsarbetet.

Riskbedömningar ska genomföras:

- om riskbedömning ska genomföras enligt lag, exempelvis Dataskyddsförordningen (GDPR)
- vid upphandling samt ny- och vidareutveckling av informationssystem
- då förändringar i arbetsprocesser leder till att hanteringen av information påverkas
- vid förhyrning, byggnation och förändring av lokaler där information som Region Skåne ansvarar för ska förvaras, behandlas eller överföras, oavsett vem som äger lokalen
- före inköp av tjänster som innebär att extern leverantör förvarar, behandlar eller på annat sätt får insyn i information tillhörande Region Skåne
- inför beslut om förändringar i den tekniska infrastrukturen
- för att hitta rätt ambitionsnivå i kontinuitetsplaner
- då det annars är påkallat

Om lagstiftning ställer krav att riskhantering ska genomföras innan information får börja hanteras eller behandlas får informationen inte hanteras eller behandlas innan riskhantering är klar och beslutade åtgärder är genomförda.

I bilaga 1 anges de skalor för sannolikhet och konsekvens som ska tillämpas vid riskanalyser inom informationssäkerhetsområdet.

Vid genomförandet ska denna instruktion och anvisning ”Riskhantering informationstillgångar” följas.

---

[1] Enligt Region Skånes ”Verksamhetstyrd styr- och förvaltningsmodell för IT- och medicintekniska system”.

7.1 Beslut om riskbehandling

Riskhanteringen omfattar beslut om hur en risk ska hanteras, vilket kallas riskbehandling. I beslutet, som ska vara skriftligt, ska den riskbedömning som är gjord med medföljande åtgärdsförslag ingå. I beslutet ska också ingå att bedöma om eventuella kvarstående risker är acceptabla eller inte. Risker i kategori A är aldrig acceptabla och ska åtgärdas, se tabell med acceptansnivåer i bilaga.

I valet av mest lämpliga riskbehandlingsåtgärder ska kostnader och insatser för implementering vägas mot bland annat rättsliga krav och patientsäkerhet. Vid val av åtgärder som kan påverka andra delar av organisationen ska denna påverkan framgå i beslutet.

Beslutet om vilka åtgärder som ska vidtas fattas av informationsägaren.

8 Dokumentation och rapportering

Informationssäkerhetschefen ska vid begäran få del av all dokumentation relaterat till riskhanteringen.

Riskanalyser som rör informationssystem för behandling av personuppgifter inom hälso- och sjukvård (patientuppgifter) kan behöva redovisas i Patientsäkerhetsberättelsen enligt Socialstyrelsens föreskrifter[2]. Riskanalyser ska i samband med detta delges Region Skånes regionala chefläkare samt i vissa fall förvaltningens chefläkare och informationssäkerhetssamordnare.

[2] Föreskrifterna och allmänna råden (7 kap. 6 § 2, HSLF-FS 2016:40) om journalföring och behandling av personuppgifter inom hälso- och sjukvården.

Bilaga 1 – Bedömningsskalor

Följande skalor ska användas vid riskbedömning av informationstillgångar.

Skala för bedömning av konsekvens

Nivå/ Skala	Bedöm-ning	Beskrivning	
1	Ingen/ Försumbar	**a) Övergripande** Ingen/försumbar skada för verksamheten/Region Skåne, annan myndighet eller enskilda fysiska eller juridiska personer.	**b) Invånare/Medarbetare** Ingen eller försumbar påverkan på liv, hälsa, rättigheter.
			c) Verksamhet/Process Ingen eller försumbar negativ effekt på verksamhetens/Region Skånes förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.
			d) Ekonomi Ingen märkbar skadekostnad för verksamheten/ Region Skåne.
			e) Förtroende Ingen/försumbar förtroendeskada för verksamheten/Region Skåne.
2	Måttlig	**a) Övergripande** Måttlig skada för verksamheten/Region Skåne, annan myndighet eller enskilda fysiska eller juridiska personer. (Kan hanteras i det löpande arbetet.)	**b) Invånare/Medarbetare** Viss påverkan på liv, hälsa, rättigheter.
			c) Verksamhet/Process Viss negativ effekt på verksamhetens/ Region Skånes förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.
			d) Ekonomi Viss skadekostnad för verksamheten/Region Skåne.
			e) Förtroende Måttlig förtroendeskada för verksamheten/Region Skåne.
3	Betydande/ allvarlig	**a) Övergripande** Betydande/allvarlig skada för verksamheten/Region Skåne, annan myndighet eller enskilda fysiska eller juridiska personer.	**b) Invånare/Medarbetare** Stor påverkan på liv, hälsa, rättigheter.
			c) Verksamhet/Process Betydande negativ effekt på verksamhetens/ Region Skånes förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.
			d) Ekonomi Betydande skadekostnad för verksamheten/Region Skåne.
			e) Förtroende Betydande/allvarlig förtroendeskada för verksamheten/Region Skåne.
4	Mycket allvarlig/ katastrof	**a) Övergripande** Mycket allvarlig/ katastrofal skada, skada för rikets säkerhet för verksamheten/Region Skåne, annan myndighet eller enskilda fysiska eller juridiska personer om den inträffar.	**b) Invånare/Medarbetare** Mycket stor påverkan på liv, hälsa, rättigheter (skadade eller dödsfall).
			c) Verksamhet/Process Mycket stor negativ effekt på verksamhetens/ Region Skånes förmåga att uppnå sina mål eller fullgöra sina primära uppgifter.
			d) Ekonomi Mycket stor skadekostnad för verksamheten/Region Skåne.
			e) Förtroende Mycket allvarlig/katastrofal förtroendeskada för verksamheten/Region Skåne.

Skala för bedömning av sannolikhet

Nivå/ Skala	Bedömning	Beskrivning
1	Mycket liten	Det finns mycket få eller inga tecken på att risken är verklighet i dag.
2	Liten sannolikhet	Inträffar sannolikt inte under normala omständigheter och i vart fall inte frekvent. Det finns vissa tecken på att risken är verklighet i mindre omfattning i dag.
3	Stor sannolikhet	Kan mycket väl inträffa men troligtvis inte särskilt frekvent. Det finns tydliga tecken på att risken är verklighet i vissa delar av verksamheten redan i dag.
4	Mycket stor sannolikhet	Sannolikheten är stor att det ska inträffa. Det är bekräftat att risken är verklighet i väsentliga delar av verksamheten redan i dag eller att den väntas bli det i närtid.

Riskmatris

Riskmatrisen visar visuellt i vilken kategori en risk har med utgångspunkt i sannolikheten att risken inträffar och konsekvenserna. Färgerna i matrisen motsvarar de acceptansnivåer som återfinns nedan.

Riskmatris			Konsekvens			
			Ingen/ Försumbar	Måttlig	Betydande/ allvarlig	Mycket allvarlig/ katastrof
			1	**2**	**3**	**4**
Sannolikhet	Mycket stor	**4**	M	H	MH	MH
	Stor	**3**	L	M	H	MH
	Liten	**2**	L	M	M	H
	Mycket liten	**1**	ML	L	L	M

Acceptansnivåer

Acceptansnivåerna anger när en risk ska åtgärdas.

Kategori MH	Mycket höga risker som kräver åtgärd. Dessa risker är inte acceptabla.
Kategori H	Höga risker som kräver åtgärd så snart som möjligt. Riskerna kan accepteras men ska bevakas.
Kategori M	Medium risker som kan behöva analyseras djupare. Riskerna bör åtgärdas och ska bevakas.
Kategori L	Låga risker som inte kräver åtgärd. Riskerna behöver inte åtgärdas men bör bevakas.
Kategori ML	Mycket låga risker som inte kräver någon åtgärd. Risk kan accepteras. Risker i denna kategori kan tillåtas öka i riskvärde om möjligheter därmed kan tillvaratas.