Beslutad av: regionstyrelsen, 2018-12-11 § 349
Diarienummer: RS 2018-00129
Giltighet: från 2019-01-01 till 2023-12-31

Riktlinje

Informationssäkerhet

Riktlinjen gäller för: Västra Götalandsregionen
Innehållsansvar: Koncernstab utförarstyrning och samordning, enhet säkerhet och beredskap

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

Inledning

Den regionövergripande dokumentstrukturen för säkerhet- och beredskapsarbetet tar sin utgångspunkt i Västra Götalandsregionens (VGR) policy för säkerhet och beredskap. Policy för säkerhet och beredskap anger värderingar, förhållningssätt och principer för arbetet med säkerhet och beredskap i Västra Götalandsregionen. Policyn lägger grunden för styrande dokument/styrning på en mer detaljerad nivå; regionstyrelsens (RS) riktlinjer för krisberedskap, informationssäkerhet, civilt försvar samt verksamhetsskydd. Riktlinjerna anger förutsättningarna för arbetet med säkerhet och beredskap i VGR. Till riktlinjerna kopplas i sin tur rutiner/planer på tjänstemannanivå, såväl regiongemensam nivå som förvaltningsnivå, samt skrivningar i reglementen och ägardirektiv.

Utgångspunkter för informationssäkerhet

Information är en av VGR:s viktigaste tillgångar och är en förutsättning för att kunna bedriva verksamhet. Riktlinje för informationssäkerhet är regionövergripande ram för området och utgår från standarden för informationssäkerhet ISO 27 000. För ett framgångsrikt arbete med informationssäkerhet ska en följsamhet mot standarden upprätthållas.

Nämnder och styrelser ansvarar för att information behandlas och skyddas på ett ändamålsenligt sätt, samtidigt som tillgången till information och öppenhet säkerställs enligt offentlighetsprincipen. Nämnder och styrelser ansvarar för hantering av informationssäkerhetsincidenter.

Skyddsområden informationssäkerhet

Det övergripande målet för informationssäkerhet är att rätt och riktig information ska nå rätt mottagare i rätt tid och vara skyddad för obehörig åtkomst och förstörelse. Skyddsområden och arbetet med informationssäkerhet syftar till att upprätthålla:

- **Tillgänglighet**: Information kan utnyttjas efter behov i förväntad utsträckning och inom önskad tid.
- **Konfidentialitet**: Information är tillgänglig endast för den medarbetare som är behörig att ta del av den.
- **Riktighet**: Skydd av information så att den är och förblir korrekt och fullständig.
- **Spårbarhet:** Hanteringen av informationstillgången är spårbar.

Förteckning över informationssystem

Nämnder och styrelser ansvarar för att det finns en förteckning över informationssystem inom sitt område. Förteckningen ska bland annat innehålla beskrivning av innehåll, syfte, ändamål, informationsägare och systemägare.

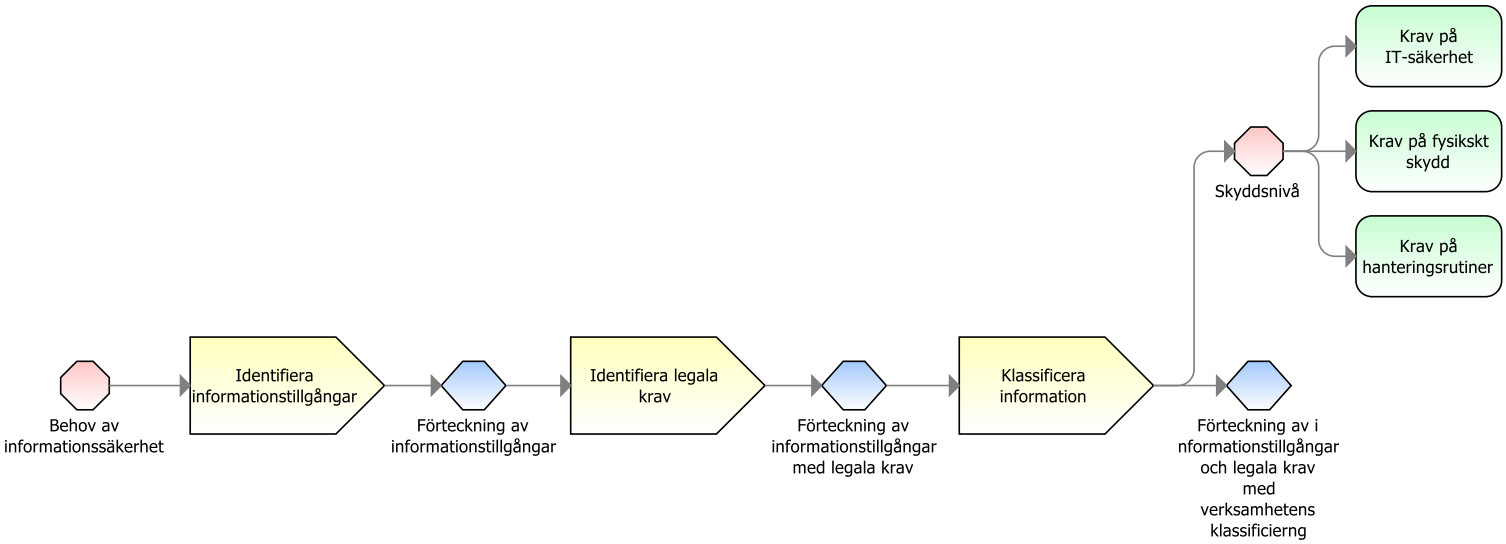
Informationsklassning

Nämnder och styrelser ska klassificera sina informationstillgångar, i syfte att avgöra lämpliga skyddsåtgärder. Skyddsåtgärderna ska skydda informationen på rätt sätt utifrån perspektiven riktighet, konfidentialitet och tillgänglighet. Klassificering av information ska genomföras vid förändringar i organisation, process och teknik samt etablering av nya IS/IT-system eller

IS/IT-tjänster som kan påverka informationshanteringen. Rutin ska finnas för märkning av handlingar med detaljerade anvisningar hur klassning av information ska genomföras.

I VGR klassificeras information i fyra klasser och informationens skyddsbehov avgör skyddsnivå. Information som har ett utökat skyddsbehov och är kopplat till hot mot Sveriges säkerhet hanteras i särskild ordning enligt säkerhetsskyddslagen.

Följande bild illustrerar processen vid klassning av information.



Modell för informationsklassning

Följande modell utgår från Myndigheten för samhällsskydd- och beredskaps mall och ska användas vid informationsklassificering inom VGR.

Konsekvensnivå	Konfidentialitet	Riktighet	Tillgänglighet	Spårbarhet	Vägledning
(Skyddsnivå) 1 Baskrav	Allmän information som om den sprids till obehöriga kan medföra försumbara konsekvenser för organisation.	Information som om den ej är riktig och fullständig kan medföra försumbara konsekvenser för organisation.	Information som om den ej är tillgänglig kan medföra försumbara konsekvenser för organisation.	Information som om den ej är spårbar kan medföra försumbara konsekvenser för organisation.	Information som är allmän för publik användning OSL
(Skyddsnivå) 2 Normala krav	Intern information som om den sprids till obehöriga kan medföra måttliga konsekvenser för organisation eller enskild individ	Information som om den ej är riktig och fullständig kan medföra måttliga konsekvenser för organisation eller enskild individ	Information som om den ej är tillgänglig kan medföra måttliga konsekvenser för organisation eller enskild individ	Information som om den ej är spårbar kan medföra måttliga konsekvenser för organisation eller enskild individ	Intern information som är allmän alt. sekretessbelagd enligt OSL.
(Skyddsnivå) 3 Höga krav	Känslig information som om den sprids till obehöriga kan medföra allvarliga konsekvenser för organisation eller enskild individ	Viktig information som om den ej är riktig och fullständig kan medföra allvarliga konsekvenser för organisation eller enskild individ	Viktig information som om den ej är tillgänglig kan medföra allvarliga konsekvenser för organisation eller enskild individ	Viktig information som om den ej är spårbar kan medföra allvarliga konsekvenser för organisation eller enskild individ	Känslig information exv. journaler, patientuppgifter enligt gällande lagstiftning och socialstyrelsens föreskrifter. Sekretess enligt OSL
(Skyddsnivå) 4 Mycket höga krav	Kritisk information som om den sprids till obehöriga kan medföra mycket allvarliga/katastrofala konsekvenser för organisation eller enskild individ	Kritisk information som om den ej är riktig och fullständig kan medföra mycket allvarliga/katastrofala konsekvenser för organisation eller enskild individ	Kritisk information som om den ej är tillgänglig kan medföra mycket allvarliga/katastrofala konsekvenser för organisation eller enskild individ	Kritisk information som om den ej är spårbar kan medföra mycket allvarliga/katastrofala konsekvenser för organisation eller enskild individ	Mycket känslig information exv. journaler, patientuppgifter enligt gällande lagstiftning och Socialstyrelsens föreskrifter. Sekretess enligt OSL, skyddad information enl. SäkL

Åtkomst till information

Nämnder och styrelser ska ansvara för att behörighet till informationstillgångar ges restriktivt och styras utifrån krav som arbetssituationen kräver. Styrning av åtkomst till patientdata syftar till att endast den som deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården kan ta del av dem.
För IS/IT-baserade system ska det finnas skyddsåtgärder mot oönskad programkod och obehörigt nyttjande. Ett fåtal medarbetare ska ha särskild behörighet och åtkomst till källprogramarkiv, operativsystem, systemhjälpmedel och revisionshjälpmedel.

Utbildning

Nämnder och styrelser ansvarar för att medarbetare regelbundet får utbildning om vilka regler som gäller vid hantering av information.

Upphandling och inköp av IS/IT system

Nämnder och styrelser ansvarar för att informationssäkerhetskraven säkerställs vid upphandling eller vid ny- och vidareutveckling av IS/IT-system. Kraven ska säkerställas och följas upp utmed systemets hela livscykel. Information med särskilda skyddsbehov, efter en genomförs risk- och sårbarhetsanalys/ informationsklassning, ska hanteras genom säkerhetsskyddsavtal med leverantörer och underleverantörer innan de beviljas åtkomst till VGR:s informationstillgångar.

Portallagstiftning

- Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1174)
- Hälso- och sjukvårdslagen (2017:30)
- Patientdatalagen (2008:355)
- Dataskyddsförordningen
- Arkivlagen (1990:782)

Definitioner

Behörighet	En persons åtkomsträttigheter till information i IT-system
Informationssäkerhet	Säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet samt spårbarhet (även oavvislighet).
Informationstillgång	En organisations information och de resurser som används för att hantera informationen.

Behörighet	En persons åtkomsträttigheter till information i IT-system
Informationsägare	Den aktör som ansvarar för informationen. Informationssägarskapet definieras och utses i respektive organisation. Respektive nämnd och styrelse företräder regionen inom sitt ansvarsområde, som informationsägare, och ansvaret följer ordinarie linjeansvar.
Konfidentialitet	Avsikten att innehållet i ett informationsobjekt, ibland även dess existens, inte bör göras tillgängligt eller avslöjas för obehöriga.
Riktighet	Egenskapen att skydda exaktheten och fullständigheten gällande tillgångar.
Tillgänglighet	Skyddsmål där informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid.
Spårbarhet	Åtgärder som kan härledas till en användare i informationssystem som är helt eller delvis automatiserade.