

Riktlinje

Fastställt av: Regionstyrelsen

Handläggare: Elena Collin

Organisation gäller inom: Region Västerbotten

Cybersäkerhet - roller och ansvar

Beslut och giltighetstid

Beslutad av Regionstyrelsen 20261020

Diarienummer: RS 724-2026

Förändringar från föregående utgåva

Ej tillämbart, första utgåva.

Omfattning

Denna riktlinje beskriver ansvar och roller för cybersäkerhetsarbetet inom Region Västerbotten och riktar sig till alla inom Region Västerbotten.

Bakgrund

Med anledning av Cybersäkerhetslagen (2025:1506) och Myndigheten för civilt försvars föreskrifter och allmänna råd om säkerhetsåtgärder och ledningens utbildning för väsentliga och viktiga verksamhetsutövare (MCFFS 2026:11) revideras tidigare fastställd styrning angående roller och ansvar inom cybersäkerhet (tidigare benämnt informationssäkerhet).

Syfte

Syftet med riktlinjen är att fastställa roller, ansvar och mål med cybersäkerhetsarbetet.

Lagar och andra krav

Cybersäkerhetslag (2025:1506)

MCFFS 2026:11

ISO/IEC 27001:2022

ISO/IEC 27002:2022

Ansvar och befogenheter

Regionfullmäktige

Regionfullmäktige har det övergripande ansvaret för cybersäkerhetsarbetet i regionen och ska

Ett utskrivet dokument är endast en kopia. Giltig version finns i ledningssystemet.

fastställa policy.

Regionstyrelse

Regionstyrelsen har utifrån reglementet i uppgift att styra och samordna förvaltningen av regionens angelägenheter och har uppsikt för hela regionens utveckling och ekonomiska ställning.

Regionstyrelsen ska ta initiativ till utveckling av arbetsformer, system och rutiner samt har även det övergripande ansvaret att se till att verksamheten arbetar i enlighet med de av fullmäktige beslutade dokument.

Regionstyrelsen har vidare ansvar för de informationssystem som stödjer regionens verksamhet och utifrån detta ansvar säkerställa att riktlinjer för cybersäkerhet finns i verksamheten samt att dessa följs.

Regionstyrelsen definieras som ledning i Cybersäkerhetslagen och ansvarar för att styra organisationens cybersäkerhetsarbete så att det bedrivs systematiskt och riskbaserat. Regionstyrelsen ska besluta om mål, inriktning och resurser, fastställa mandat och tillse att organisationen har tillräcklig kompetens och tillräckliga resurser för att nå den säkerhetsnivå som krävs. Regionstyrelsen ansvarar för att tydliggöra roller och ansvar för att all information och alla system har ägare som tar ansvar för säkerheten utifrån sina roller. Regionstyrelsen ska säkerställa att det finns roll och ansvar för samordning av cybersäkerhetsarbetet för att tillse de får dom underlag som behövs för att styra cybersäkerhetsarbetet. Regionstyrelsen ska genomgå utbildning om säkerhetsåtgärder samt ansvarar för att minst en gång per år genomföra ledningens genomgång och besluta om säkerhetsåtgärder.

Styrelse och nämnder

Styrelsen och nämnderna är personuppgiftsansvarig enligt definitionen i 3 § dataskyddsförordningen. I detta ingår ansvar för att regionens arbete med cybersäkerhet sker på ett ändamålsenligt sätt och i enlighet med fastställda riktlinjer inklusive att nödvändiga resurser avsätts för att förebygga och hantera incidenter.

Objektägare

All information som skapas inom regionen skall ha en ägare. **Objektägare är informationsägare** i enlighet med cybersäkerhetslagen för informationen som hanteras inom de system som hen är objektägare för. Objektägaren har ansvaret för att säkerställa att lämpliga och proportionella säkerhetsåtgärder är vidtagna för informationsbehandlingen vid anskaffning, utveckling, underhåll och avveckling. Detta innebär att informationen är värderad, risker analyserats samt utifrån detta bedöma vilken nivå av skydd utifrån konfidentialitet, riktighet inklusive autenticitet och tillgänglighet som behövs. All information ska informationsklassificeras och säkerhetsåtgärder ska systematiskt arbetas

Ett utskrivet dokument är endast en kopia. Giltig version finns i ledningssystemet.

med utifrån genomförd klassning.

Objektägaren ansvarar för att inhämta och dokumentera nivå av skydd för informationen samt acceptabla tider för otillgänglighet. Objektägare ska informera Objektägare teknik om identifierad nivå av skydd för informationen samt acceptabla tider för otillgänglighet och bristande funktionalitet för informationsbehandlingen. Objektägare ansvarar för framtagande av kontinuitetsplaner för systemet, samt att de testas, följs upp och revideras regelbundet.

Objektägare teknik

Alla system som hanteras inom regionen ska ha en systemägare. **Objektägare teknik är systemägare** i enlighet med cybersäkerhetslagen för de system som hanteras inom det objekt hen är objektägare teknik för. Objektägare teknik ansvarar för att säkerställa att risker har analyserats och att Objektägarens (informationsägarens) identifierade nivå av skydd uppnås i berörda system. Objektägare teknik ska informera berörd Objektägare om brister i systemens cybersäkerhet som påverkar informationsbehandlingen. Objektägare teknik ska säkerställa att systemen under hela deras livslängd är skyddade med lämpliga och proportionella säkerhetsåtgärder utifrån genomförd informationsklassning och identifierade risker.

Objektstyrning

Utveckling och förvaltning av regionens system sker i enlighet med regionens objektmodell. Varje system i regionen skall ha en objektägare och en objektägare teknik. Alla system ska vara tilldelade ett objekt. Om system tillfälligt inte har ett tilldelat objekt är det verksamhetschef i den verksamhet som införskaffat systemet som är både informationsägare och systemägare, och ansvarar för att lämpliga och proportionella säkerhetsåtgärder vidtas på samma sätt som om systemet tillhört ett objekt.

Cybersäkerhetsstrateg säkerhetsenheten

Det systematiska och riskbaserade cybersäkerhetsarbetet ska ha en samordnare.

Cybersäkerhetsstrateg på Säkerhetsenheten är samordnare för cybersäkerhetsarbetet.

Cybersäkerhetsstrategen ansvarar för att samordna det systematiska och riskbaserade arbetet med cybersäkerhet och utvärdera nivån av cybersäkerhet i förhållande till externa krav, interna behov och identifierade risker. Cybersäkerhetsstrategen ska säkerställa att de underlag som Regionstyrelsen behöver för att godkänna och övervaka genomförandet av säkerhetsåtgärder sammanställs.

Verksamhetschef

Verksamhetschefen har det övergripande ansvaret för cybersäkerheten i verksamheten.

Verksamhetschef ansvarar för att anställda inom hens verksamhet har kunskap om fastställd styrning avseende cybersäkerhet och informationshantering i de system som används. Verksamhetschefen

Ett utskrivet dokument är endast en kopia. Giltig version finns i ledningssystemet.

har också planeringsansvar för lokala kontinuitetsplaner, samt ansvarar för att verksamhetsnära reservrutiner dokumenteras och övas och att anställda i verksamheten genomfört obligatoriska utbildningar i cybersäkerhet.

Informationsanvändare

Varje enskild person som hanterar Region Västerbottens information ansvarar för att följa gällande styrning avseende hantering av regionens information samt genomföra obligatoriska utbildningar i cybersäkerhet och rapportera incidenter.

Projekt- och uppdragsägare

Projekt- och uppdragsägare ansvarar för att leveransen uppfyller ställda krav och mottagande organisation ansvarar för att godkänna leveransen, där det tydligt behöver framgå om det finns kvarstående risker. Projekt- och uppdragsägare ansvarar för att cybersäkerhet integreras i projekt- och uppdragsledningen för att säkerställa att cybersäkerhetsrisker som rör projektet/uppdraget och dess leveranser beaktas, bedöms och hanteras under projektets/uppdragets livscykel.

Beskrivning/Genomförande

Region Västerbotten ska utveckla och bedriva ett systematiskt och riskbaserat cybersäkerhetsarbete med stöd av ISO 27000-standarden om ledningssystem för informationssäkerhet, cybersäkerhet och integritetsskydd. Tekniska, organisatoriska, fysiska och personrelaterade säkerhetsåtgärder ska vidtas för att skydda regionens information utifrån konfidentialitet, riktighet och tillgänglighet.

Anställda inom Region Västerbotten ska få tillräcklig information om sina tilldelade roller och ansvar och ha tillgång till styrande dokument som beskriver förväntningar för respektive roll kopplat till cybersäkerhet. Regionens anställda ska ha befogenhet att uppfylla organisationens styrande dokument och ha kompetens i fråga om cybersäkerhet.

Mål

Cybersäkerhetsarbetets önskade tillstånd är att informationen alltid ska finnas tillgänglig när den behövs, att informationen är korrekt och att endast behöriga har åtkomst. Det önskade tillståndet inkluderar ett antal mål som vi ska arbeta för att nå och upprätthålla:

1. *Region Västerbotten ska bedriva ett systematiskt och riskbaserat cybersäkerhetsarbete som säkerställer att cybersäkerhetsrisker identifieras, bedöms, hanteras och följs upp.*
2. *Region Västerbotten ska genom utbildning, medvetandegörande och övning stärka en riskmedveten säkerhetskultur som genomsyrar styrning, beslut och dagligt arbete.*
3. *Region Västerbotten ska under hela informationssystemens livscykel identifiera och hantera säkerhetsrisker i leverantörskedjan samt vid anskaffning, utveckling, förändring och avveckling av informationssystem.*
4. *Region Västerbotten ska upptäcka, hantera och rapportera incidenter samt upprätthålla kontinuitet och säkerställa återställningsförmåga i kritiska verksamheter.*

Dokumentation och arkivering

Ej tillämbart.

Historik

Ersätter delar av tidigare fastställt dokument: Informationssäkerhet - förvaltning och drift

Referenser

Riktlinjer i ledningssystemet för Riskhantering och för Anskaffning, utveckling och förändring av informationssystem.

Utarbetat av

Cybersäkerhetsstrateg på Säkerhetsenheten i samråd med kompetenser inom området.

Dokumentinformation

Här anges information om vad som finns i grå ruta, sidhuvud, sidfot och om information angetts om kontrollerade kopior. Det anges här för att kunna läsas av hjälpmedel för synnedsatta.

Denna information får inte tas bort!

Information i sidhuvud

Bild på region Västerbottens logga.

Versionsnummer: 0.6

Giltigt från och med:

Uppföljningsdatum:

Information i grå ruta på första sidan

Dokumenttyp: Riktlinje

Fastställt av: Regionstyrelsen

Handläggare: Elena Collin

Organisation gäller inom: Region Västerbotten

Information i Sidfot

Dokumentnummer: 103085

Kontrollerade kopior