region västerbotten

Tjänsteskrivelse
2025-11-17

Sofia Gustafsson
Säkerhet

Revidering av ledningens ansvar med anledning av nya cybersäkerhetslagen

RS 855-2025

Sammanfattning

Den nya cybersäkerhetslagen träder i kraft den 15 januari 2026. Lagen innebär ett förtydligat och utökat ansvar för ledningen att säkerställa att verksamheten bedriver ett systematiskt och riskbaserat arbete med cybersäkerhet. Syftet med lagen är att stärka samhällets motståndskraft mot cyberhot och att skapa en enhetlig reglering av cybersäkerhet inom både offentlig och privat sektor. Lagen ställer ökade krav på styrning, riskhantering och rapportering av IT- och informationssäkerhetsincidenter. Lagen syftar också till att säkerställa att verksamheter som bedriver samhällsviktiga tjänster ska arbeta med systematiska och riskbaserade säkerhetsåtgärder.

Föreskrifterna om anmälningsskyldighet föreslås även de träda i kraft den 15 januari 2026, vilket innebär att organisationer som omfattas av lagen ska kunna anmäla relevanta verksamheter och kontaktuppgifter till ansvarig myndighet från detta datum. Region Västerbotten kommer att omfattas av denna anmälningsskyldighet.

Föreskrifter som rör utbildning och säkerhetsåtgärder samt incidentrapportering och informationsskyldighet förväntas träda i kraft under mars 2026. Det innebär att verksamheterna får en övergångsperiod för att anpassa sina interna processer och säkerhetsrutiner till de nya kraven.

En viktig förändring i den nya lagstiftningen är att ledningsansvaret tydliggörs och fastställs till regionstyrelsen för respektive region. Det innebär att den högsta ledningen i organisationen, det vill säga regionstyrelsen, bär det yttersta ansvaret för att säkerställa att verksamheten uppfyller lagens krav på cybersäkerhet. Den nya cybersäkerhetslagen innebär ett tydligare ansvar för ledningen i varje organisation som omfattas av lagen. Ledningen har det övergripande ansvaret för att:

- säkerställa att organisationen bedriver ett systematiskt och riskbaserat cybersäkerhetsarbete
- fatta nödvändiga strategiska beslut för att uppfylla lagens krav
- tillse att resurser och kompetens finns för att genomföra säkerhetsåtgärder
- följa upp att styrning, intern kontroll och rapportering sker enligt lagens föreskrifter

Detta innebär att cybersäkerhet ska ingå i det övergripande ledningsansvaret och styrningen av regionens verksamhet. Regionens arbete med cybersäkerhet ska omfatta tekniska, organisatoriska, personella och fysiska säkerhetsåtgärder.

För att efterfölja den nya cybersäkerhetslagen och dess föreskrifter måste ledningen genomgå

utbildning, regionen måste anmäla sig som verksamhetsutövare till berörd till tillsynsmyndighet samt upprätta rutiner för incidentrapportering.

Förslag till beslut
Regionstyrelsen föreslås fatta följande beslut:

- Regiondirektören uppdras, med rätt att vidaredelegera, att vidta de åtgärder som behövs för att säkerställa att Region Västerbotten uppfyller kraven i den nya cybersäkerhetslagen och tillhörande föreskrifter, inklusive anmälningsskyldighet, utbildningsinsatser, säkerhetsåtgärder samt rutiner för incidentrapportering och informationshantering.

Bedömda resultat och konsekvenser
Genom att anpassa regionens arbete till den nya cybersäkerhetslagen stärks det systematiska och riskbaserade arbetet inom informations- och cybersäkerhet. På kort sikt bedöms införandet medföra ett ökat resursbehov för utbildning, styrning och genomförande av säkerhetsåtgärder inom samtliga verksamheter. På längre sikt förväntas åtgärderna bidra till en mer motståndskraftig och robust organisation, där informations- och cybersäkerhet utgör en integrerad del av regionens lednings- och styrningsprocesser.

Bristande efterlevnad av lagens krav kan leda till tillsynsåtgärder från ansvarig myndighet och sanktionsavgifter samt innebära ökade risker för driftstörningar, informationsförluster och minskat förtroende för regionens förmåga att leverera samhällsviktiga tjänster.

Resurser och finansiering
Implementering av cybersäkerhetslagen och dess föreskrifter innefattas i regionens verksamhetsansvar och finansiering för relaterat arbete ligger inom ramen för verksamheternas budget.

Jämställdhet

Cybersäkerhetsarbetet bedrivs könsneutralt. Ledningen bör beakta att beslut och prioriteringar inom området kan ha påverkan ur ett jämställdshetsperspektiv och därför bör framtida analyser inkludera detta perspektiv.

Beredningsansvariga
- Sofia Gustafsson, cybersäkerhetsstrateg
- Johan Tegström, arkitekt digitalisering och IT-säkerhetsansvarig
- Jonas Andersson Sjukhusfysiker och cybersäkerhetsstrateg
- Henrik Sandberg, regionjurist

Beslutsunderlag

-

Beslutet expedieras till
Säkerhetsenheten