Policy för informationssäkerhet, cybersäkerhet och integritetsskydd

INLEDNING

I varje organisation finns det mängder av information som behövs för att bedriva och utveckla verksamhet och förvalta organisationen.

Informationshantering innebär hela informationstillgångens livscykel så som att samla in, organisera, redovisa, tillhandahålla, kommunicera, lagra, använda, destruera och arkivera informationen. Informationen ska användas på ett ändamålsenligt, kontrollerat och säkert sätt.

Region Västmanlands informationshantering styrs av ett flertal nationella- och EU författningar som på olika sätt ställer krav på informationssäkerhet, cybersäkerhet och integritetsskydd.

Informationssäkerhet är teknikneutral och omfattar skydd för hela informationstillgångens livscykel oavsett informationens format, såsom i tal, på papper eller i system.

Cybersäkerhet, som även kallas informationsteknologisk säkerhet eller datasäkerhet, innebär att åtgärder införs som skyddar system och nätverk från att information avslöjas, att hårdvara, programvara eller elektroniska data stjäls eller skadas samt från att de tjänster som tillhandahålls störs eller feldirigeras. Integritetsskydd, eller dataskydd som det också ofta kallas, inbegriper skydd för varje enskild persons uppgifter.

Informationssäkerhetsarbete innefattar administrativa, tekniska och fysiska åtgärder som skyddar information mot att läcka ut, förvanskas eller förstöras.

SYFTE

Policyn ska klargöra hur regionen ska upprätthålla en god och säker informationshantering.

Policyn ska ge samtliga medarbetare en tydlig bild av de principer som ligger till grund för hur informationshantering sker på ett säkert sätt. På detta vis förblir information som regionen hanterar lagenlig och ändamålsenlig. Varje informationstillgång ska hanteras genom en avvägning mellan informationssäkerhet, effektivitet och ekonomi.

INRIKTNING OCH TILLÄMPNING

Regionens målsättning är att vara certifieringsbar enligt SS-ISO/IEC 27001. Ledningssystemet för informationssäkerhet, cybersäkerhet och integritetsskydd ska utgöra ett stöd för ledningen och verksamheten att efterleva relevanta författningskrav inom området.

Policy för informationssäkerhet, cybersäkerhet och integritetsskydd

OMFATTNING

Denna policy gäller för Region Västmanlands förvaltningar och helägda bolag. Allt informationssäkerhetsarbete ska utgå ifrån denna policy samt tillhörande riktlinjer, rutiner och instruktioner.

ANSVAR OCH ROLLER

Regionfullmäktige har det yttersta ansvaret för informationssäkerhets- och dataskyddsarbetet. Fullmäktige fattar beslut om policy och övergripande inriktning för arbetet samt tilldelar medel för genomförandet av åtgärder. Regionstyrelsen ska ha en uppdaterad lägesbild över identifierade risker som kan få en allvarlig konsekvens för regionens verksamhet och besluta om hur dessa risker ska hanteras.

Ansvaret för informationssäkerhet och dataskydd följer det ordinarie verksamhetsansvaret från regiondirektören till den enskilde medarbetaren. Detta innebär att den som är ansvarig för en viss verksamhet (klinik, avdelning, enhet, process etc.) också är ansvarig för informationssäkerhet och dataskydd inom det verksamhetsområdet och har ansvar för tillämpningen av ledningssystemets regelverk i den egna verksamheten samt framtagandet av rutiner och för verksamheten anpassade instruktioner.

Samtliga medarbetare har ansvar att följa gällande regler avseende informationssäkerhet, cybersäkerhet och dataskydd.

Informationssäkerhetsfunktionen har ansvar för att leda regionens arbete inom informationssäkerhet, ge verksamheten råd och stöd, upprätta och revidera styrdokument inom området, omvärldsbevaka inom området och upprätthålla goda och relevanta nätverk.

PRINCIPER

Regionens informationssäkerhetsarbete innebär att

- säkerställa att regionen hanterar information rättssäkert enligt gällande författningar,
- säkerställa en tillräcklig informationssäkerhet i informationssystem och nätverk,
- ge personal medvetenhet och kompetens avseende informationssäkerhet i det dagliga arbetet,
- varje informationstillgång, personuppgiftsbehandling, risk eller konsekvens ska ha en ägare som ansvarar för åtgärderna,

Policy för informationssäkerhet, cybersäkerhet och integritetsskydd

- information ska klassificeras utifrån principerna konfidentialitet, riktighet, integritetskänslighet och tillgänglighet för att i sin tur säkerställa lämpliga organisatoriska och tekniska säkerhetsåtgärder,
- vid inköp, upphandling, utveckling och förändring av funktioner i informationssystem ska informationssäkerhet alltid vara beaktad, prioriterad och implementerad, samt
- arbete med informationssäkerhet, dataskydd och kontinuitet ska implementeras av samtliga verksamheter.

INCIDENTHANTERING

Regionen ska ha en känd, säker och effektiv hantering och rapportering av informationssäkerhetsincidenter.

Regionens informationssäkerhetsarbete ska bygga på ett riskbaserat förhållningssätt. Risker ska identifieras, bedömas och hanteras genom proportionerliga åtgärder som förebygger incidenter samt begränsar deras konsekvenser.

UPPFÖLJNING

Uppföljning och revidering av regionens informationssäkerhetsarbete ska ske regelbundet och strukturerat samt baseras på interna kontroller och revisioner av oberoende part.

REFERENSER

- Tryckfrihetsförordningen (1949:105)
- Offentlighets- och sekretesslagen (2009:400)
- Patientdatalagen (2008:355)
- Hälso- och sjukvårdslagen (2017:30)
- Arkivlagen (1990:782)
- Kommunallagen (2017:725)
- Förvaltningslagen (2017:900)
- Dataskyddsförordningen (EU 2016/679)
- Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
- NIS2-direktivet (EU 2022/2555)
- Cybersäkerhetslag (2025:1506)
- SS-EN ISO 27000-serien

Policy för informationssäkerhet, cybersäkerhet och integritetsskydd

INTER REFERENS

Denna policy är fastställd av Regionfullmäktige [XXXX-XX-XX §XX], dnr RV 260766.