Informationssäkerhetspolicy

INLEDNING

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

Informationshantering omfattar att samla in, organisera, redovisa, tillhandahålla, kommunicera, lagra och använda 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.

SYFTE OCH MÅL

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

Policyn ska ge samtliga medarbetare en tydlig och säker struktur för hur informationshantering sker på ett rättssäkert sätt, på detta vis förblir information som regionen hanterar lagenlig och ändamålsenlig.

INRIKTNING OCH TILLÄMPNING

Regionens inriktning är att vara certifieringsbara enligt SS-ISO/IEC 27001.

OMFATTNING

Denna policy gäller för Region Västmanlands förvaltningar och helägda bolag. Policyn kompletteras av styrande dokument med beskrivningar av ansvar och aktiviteter.

Denna policy gäller all verksamhet och alla medarbetare som använder regionens information. Som medarbetare räknas även uppdragstagare och externa leverantörer.

ANSVAR OCH ROLLER

Denna policy gäller för Region Västmanlands förvaltningar och helägda bolag. Regionfullmäktige har det yttersta ansvaret för informationssäkerhetsarbetet. Fullmäktige fattar beslut om policy och övergripande inriktning för arbetet samt tilldelar medel för genomförandet av åtgärder.

Informationssäkerhetspolicy

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.

Regiondirektören och chefer har ansvar för tillämpningen av ledningssystemets regelverk i den egna verksamheten.

Samtliga medarbetare har ansvar att följa gällande regler avseende informationssäkerhet. Som anställd inom regionen utgör den en del av Sveriges offentlighetsstruktur och är en del av upprätthållandet av bland annat offentlighetsprincipen och hantering av sekretess. Information som hanteras av varje medarbetare behöver därav förhålla sig till vad som krävs vad gäller dokumentation, lagring och sekretess.

Informationssäkerhetssfunktionen har i ansvar att ge verksamheten råd och stöd, ta~~r~~ fram och reviderar styrdokument inom området, omvärldsbevaka inom området och upprätthålla goda och relevanta nätverk.

PRINCIPER

Regionens informationssäkerhetsarbete innebär att

- säkerställa att regionen hanterar information rättssäkert efter gällande lagstiftning.
- säkerställa en tillräcklig informationssäkerhet i informationssystem, nätverk, digitisering och digitalisering.
- ge personal medvetenhet och kompetens om informationssäkerhet i sitt dagliga arbete.
- varje informationstillgång, risk eller konsekvens ska ha en ägare som ansvarar för åtgärderna.
- information ska klassificeras utifrån principerna konfidentialitet, riktighet, integritet och tillgänglighet för att i sin tur säkerställa lämpliga organisatoriska och tekniska säkerhetsåtgärder.
- säker informationshantering inkluderar hela livscykeln, innefattande om hur informationen används, lagras, delas, överförs, arkiveras och raderas.
- upphandling, utveckling och förändring av funktioner ska informationssäkerhet alltid vara beaktad, prioriterad och implementerad.
- arbete med informationssäkerhet och kontinuitet ska implementeras av samtliga verksamheter.
- regionens informationssäkerhet ska utgå från en riskbaserad ansats och vidta åtgärder för att förebygga och minimera verkningar av konsekvenser.

Informationssäkerhetspolicy

- regionen ska i sitt informationssäkerhetsarbete ha en känd, säker och effektiv incidenthantering och incidentrapportering.

UPPFÖLJNING

Uppföljning av regionens arbete med informationssäkerhet ska ske på ett regelbundet och strukturerat sätt samt utföras genom 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)
- Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174)
- Dataskyddsförordningen (EU 2016/679)
- SS-EN ISO 27000-serien