Informationssäkerhetspolicy

SYFTE

Region Västmanland ska bedriva ett systematiskt arbete med informationssäkerhet som bygger på riskanalyser och ständiga förbättringar. Det ska präglas av en tydlig styrning av säkerhetsarbetet där olika typer av information omges av rätt skyddsåtgärder och att en avvägning sker mellan säkerhet, effektivitet och ekonomi.

DEFINITION

Informationssäkerhet är teknikneutralt och omfattar skydd av bland annat muntlig, pappersbunden och digital information. Skyddet gäller informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet.

INRIKTNING OCH TILLÄMPNING

Regionens inriktning är att vara certifieringsbar enligt SS-ISO/IEC 27001. Samtliga krav i standarden har bedömts tillämpliga för regionen.

OMFATTNING

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

PRINCIPER

- Risker som kan påverka regionens informationssäkerhet ska identifieras, analyseras och hanteras.
- Regionen ska ha en metod för informationsklassning som möjliggör styrning av lämpliga säkerhetsåtgärder till olika informationstillgångar.
- All information och övriga informationstillgångar ska vara kopplade till en ägare som har ansvar för att informationen och resurserna skyddas på ett adekvat sätt. Ansvaret gäller oavsett om de hanteras internt eller externt.
- Alla medarbetare ska ha tillräcklig kännedom om regionens säkerhetsregler för att kunna utföra sina arbetsuppgifter på ett säkert sätt.
- Regionens informationshantering ska utföras på sådant sätt att fysiska personers integritet skyddas vid behandling av personuppgifter.
- Drift och förvaltning av it-miljö, system och de tillhörande resurserna ska ske utifrån generella säkerhetskrav och de specifika säkerhetskrav som ställs av verksamheten genom bland annat informationsklassning.
- Åtkomst till information ska ges enligt klart definierade principer, tydliga ansvarsförhållanden och enhetliga metoder.
- Lämpliga krav på spårbarhet ska finnas omsatta i all informationshantering.

Informationssäkerhetspolicy

- Upphandling, utveckling och förändring av funktioner som kan påverka informationssäkerheten ska ske enligt en fastställd metod där säkerhetsaspekter har en framträdande roll.
- Regionen ska fastställa sina krav på informationssäkerhet och kontinuitet för styrning av informationssäkerhet vid svåra situationer, exempelvis under en kris eller katastrof.
- En process för incidentrapportering och -hantering ska finnas för att mildra effekter, förhindra upprepande och underlätta återgång till verksamhet på normal nivå då någon form av säkerhetsincident skett.

ANSVAR OCH ROLLER

Regionfullmäktige har det yttersta ansvaret för informationssäkerhetsarbetet. 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.

Regiondirektören och chefer har ansvar för tillämpningen av ledningssystemets regelverk i den egna verksamheten. Detta ansvar innebär bland annat framtagande av rutiner och instruktioner anpassade för den egna verksamheten.

Samtliga medarbetare har ansvar att följa gällande regler avseende informationssäkerhet.

Informationssäkerhetssamordnaren ansvarar för samordning och utveckling av informationssäkerhetsarbetet. Som ett stöd i detta arbete finns Informationssäkerhetsrådet med representanter för verksamheterna samt relevanta specialistfunktioner.

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.

INTERN REFERENS

Denna policy är fastställd av Regionfullmäktige 2019-XX-XX § 11, dnr RV XXXXX.