Dokumentansvarig
Informationssäkerhetsenheten
Jonas Jensen
Avser
Processområde: Hantera information
Beslutad av
Regionfullmäktige den 23 november 2021, § 131/21

Giltig från
2021-11-23

Dokumentnummer
RS-LED20-3246-4

Dokumentkategori
Huvuddokument (styrande dokument)

Informationssäkerhetspolicy

Inledning

Region Sörmlands verksamhet ska utgå från principerna om öppenhet, personlig integritet och respekt för individen. Medborgarna ska möjliggöras insyn i verksamheten och kunna förlita sig på regionens hantering av sin information och skydd av denna.

Digitalisering av processer och verksamhet och en utveckling med informationshantering i informationssystem och nya funktioner innebär stora förbättringar i många avseenden. Det innebär också att beroendet till informationssystem och att sårbarheten och riskexponeringen ökar om inte säkerhetsaspekterna beaktas.

Information är en av regionens mest kritiska resurser. Hela verksamheter är beroende av information. Avbrott i tillgången till information och felaktig information kan orsaka allvarliga konsekvenser i verksamheten eller för enskilda individer.

Syfte

Denna policy beskriver de övergripande principer som ska gälla för informationssäkerhetsarbetet i Region Sörmland.

Informationssäkerhetspolicyn gäller för hantering av all information, i alla dess former i Region Sörmland inklusive bolag och stiftelser och för de som arbetar på uppdrag av regionen. Det sistnämnda regleras genom avtal.

Informationssäkerhetsarbetet styrs av regionens ledningssystem för informationssäkerhet utformat utifrån ISO/IEC 27000 och organisationens verksamhetskrav samt gällande författningar.

Ledningssystemet består av styrande dokument som utgörs av denna policy med tillhörande riktlinjer och eventuella tillämpningsanvisningar.

Eventuellt verksamhetsspecifika styrande dokumenten ska utformas utifrån de regiongemensamma.

Metodstöd och manualer är inte styrande utan utgör stöd och metod för att utföra informationssäkerhets- och dataskyddsåtgärder.

Mål

Regionens informationssäkerhetsarbete ska skydda informationen inom verksamheten mot yttre och inre hot. Skyddet ska vara anpassat till skyddsvärdet, risk och lagkrav och därigenom möjliggöra för regionens verksamheter att uppnå sina mål. Följande mål är styrande för informationssäkerheten i regionen.

- **Säker och riskbaserad informationshantering**
  Informationstillgångar klassificeras och riskbedöms samt hanteras utifrån dess skyddsbehov, så att den är riktig och tillgänglig när den behövs och skyddas mot obehörig åtkomst. Detta för att värna verksamhetens förmåga att utföra sitt uppdrag och skydda individer mot skada. Lika viktigt är att värna integriteten för medborgarna. Medborgarna ska känna trygghet i att regionen omhändertar deras intressen avseende integritet och säkerhet i behandlingen av deras uppgifter.

- **God informationssäkerhetskultur**
  Behovet av skydd av information bedöms och är en central del i arbetet på alla nivåer i verksamheten utifrån de risker och hot som finns mot informationen och medarbetare är medvetna om sitt ansvar som användare.

- **Effektiv incidenthantering**
  Regionen har förmåga att hantera och lära av allvarliga informationssäkerhetsincidenter.

- **Robust informationshantering**
  Verksamheternas informationssystem och IT-infrastrukturen är riskbedömda och kontinuitetsplanerad där åtgärder som ska vidtas vid avbrott, störningar och kriser är planerade, testade och övade.

- **Informationssäkerhetsberättelse**
  Ledningen och regionstyrelsen ska informeras av särskild utsedda roller om informationssäkerhetsläget och dataskydd i regionen samt om vilka åtgärder som bör vidtas.

- **Handlingsplan**
  Handlingsplan för informationssäkerhet ska beslutas av regionstyrelsen.

Ansvar

Regionfullmäktige fastställer informationssäkerhetspolicy för regionen.

Regionstyrelsen ansvarar för att informationssäkerhetspolicy och riktlinjer för informationssäkerhet utarbetas och hålls aktuella. Regionstyrelsen beslutar om riktlinjer för informationssäkerhet och följer upp handlingsplan med mätbara mål för informationssäkerhet.

Regionstyrelsen är ansvarig för informationssäkerhet och personuppgiftshanteringen inom hela regionen förutom folktandvården vars styrelse själv är ansvarig. Inom ramen för regionens ledningssystem ska det antas verksamhetsspecifika styrdokument för informationssäkerhet och personuppgiftshanteringen där så är nödvändigt. Det åligger regionstyrelsen och bolagsstyrelsen att årligen följa upp informationssäkerheten och personuppgiftshanteringen.

Ansvaret för informationssäkerheten är generellt kopplat till det delegerade verksamhetsansvaret.

Uppföljning

Uppföljning och revidering av denna policy ska ske i enlighet med Region Sörmlands styrmodell och hantering av styrande dokument.

Uppföljning av följsamhet gentemot denna policy med tillhörande riktlinjer och anvisningar ska kontrolleras årligen och rapporteras till regiondirektör, regionstyrelse och bolag.

Versionshantering

Datum	Kommentar
2015-03-03	Utgåvan fastställd, landstingsfullmäktige den 3 mars, § 11/15
2018-12-31	Justering av namn och grafisk profil inför regionbildning, landstingsfullmäktige den 6 mars, § 8/18
2020-12-10	Justering utifrån tillgänglighetskrav, WCAG 2.1
2021-10-06	Mindre justering av ansvar för personuppgiftsbehandling på nämndnivå och användning av ny mall.