

Policy för informationssäkerhet och dataskydd

Om policy för informationssäkerhet och dataskydd

Denna policy för informationssäkerhet och dataskydd anger inriktning och mål för arbetet med informationssäkerhet och dataskydd inom Region Jönköpings Län. Policyn omfattar all informationshantering inom Region Jönköpings län och konkretiseras i verksamhetsövergripande riktlinjer och regelverk.

Syfte

Information och personuppgifter är av grundläggande betydelse och en av de viktigaste tillgångarna för Region Jönköpings läns verksamheter. En säker hantering av information och personuppgifter är en förutsättning för att Region Jönköpings län ska nå sina verksamhetsmål med ett bibehållet förtroende från allmänheten. Syftet med policyn för informationssäkerhet och dataskydd är att Region Jönköpings län ska fullfölja sina åtaganden i enlighet med gällande lagar samt uppsatta mål, aspekter och principer vad gäller informationssäkerhet och dataskydd.

Mål

Målet med policyn för informationssäkerhet och dataskydd är att arbetet ska bedrivas på ett systematiskt och riskbaserat sätt med ständiga förbättringar samt värna om medborgarnas fri- och rättigheter. Region Jönköpings län ska arbeta utifrån framtaget ledningssystem för informationssäkerhet och dataskydd (LISD) som utgår från den internationella standardserien SS-ISO/IEC 27000 samt följa gällande dataskyddslagstiftning.

Aspekter och principer

Informationssäkerhetsaspekter

Information är en tillgång som behöver skyddas efter behov. En del av informationen är värdefull, både för organisationer och för den enskilda medborgaren. Därför behöver Region Jönköpings län skydda informationen så att:

- endast behöriga personer tar del av den (Konfidentialitet)
- den är fullständig, korrekt och inte förvanskad (Riktighet)
- den finns tillgänglig när den behövs (Tillgänglighet)
- det går att se vem som har gjort vad och när i systemen (Spårbarhet)

Dataskyddsprinciper

Region Jönköpings län ska säkerställa att personuppgiftsbehandlingar sker på ett lagligt och korrekt sätt så att:

- Endast de personuppgifter som är adekvata och relevanta för ändamålet samlas in. Detta innebär att insamlingen inte får vara mer omfattande än nödvändigt.
- Insamlade personuppgifter är korrekta och uppdaterade.
- Personuppgifterna behandlas på ett transparent sätt gentemot de registrerade.
- Insamlade personuppgifter bara bevaras så länge det är nödvändigt för ändamålet.
- Endast behöriga får åtkomst till personuppgifter.
- Personuppgifterna skyddas av lämpliga tekniska och organisatoriska åtgärder.

Ansvar och roller

En grundläggande förutsättning för att Region Jönköpings län ska uppnå målet med informationssäkerhets- och dataskyddsarbetet är en tydlig fördelning av roller och ansvar.

Informationssäkerhet

Region Jönköpings läns nämnder är var och en ytterst ansvarig för hur informationen hanteras inom regionens alla verksamheter. Regionstyrelsen har det övergripande ansvaret för informationssäkerheten och regiondirektören är regionstyrelsens verkställande tjänsteman med ansvar att ge förutsättningar för ett systematiskt och riskbaserat arbetssätt.

Ansvaret för informationssäkerheten på verksamhetsnivå följer det delegerade verksamhetsansvaret. Detta gäller från Regionledningen till den enskilde medarbetaren och innebär att den som är ansvarig för en verksamhet också är ansvarig för informationssäkerheten och för informationen som hanteras inom respektive verksamhet.

Dataskydd

Nämnderna är var och en personuppgiftsansvariga för den behandling av personuppgifter som görs inom respektive verksamhetsområde. Regionstyrelsen utser dataskyddsombud och respektive nämnd ansvarar i övrigt för frågor som ankommer på personuppgiftsansvarig enligt dataskyddsförordningen.

Dataskyddsombudet: Har en stödjande, vägledande roll i organisationen och ska tillse efterlevnad av gällande dataskyddslagstiftning. Dataskyddsombudet är kontaktperson för de registrerade, för den egna organisationen och för tillsynsmyndigheten.

Avvikelser

Varje medarbetare ska rapportera informationssäkerhets- och personuppgiftsincidenter och avvikelser från denna policy med tillhörande riktlinjer och regelverk. Incidenter och avvikelser rapporteras i enlighet med gällande incident- och avvikelseprocesser i avsett system. Erfarenheterna av

inrapporterade avvikelser och incidenter ska tas till vara och användas i det kontinuerliga förbättringsarbetet inom Region Jönköpings län.

Rapportering

Rapportering avseende informationssäkerhets- och dataskyddsarbetet sker minst årligen till regiondirektör samt till nämnderna.

Revidering

Denna policy för informationssäkerhet och dataskydd ska revideras vid behov, dock minst en gång per mandatperiod.

Policy för informationssäkerhet och dataskydd är beslutad av regionfullmäktige 2024-06-11, § 83 och gäller fr. o. m. 2024-06-11.