BÄSTA LIVSPLATSEN
Region Halland

Säkerhet - Riktlinjer för Informationssäkerhet och dataskydd

Styrande dokument för dessa riktlinjer är Regionfullmäktiges *Säkerhetspolicy* antagen 2018-xx-xx.

Syfte
Dessa riktlinjer syftar till att ge vägledning samt precisera innebörden i Region Hallands säkerhetspolicy.

Omfattning
Riktlinjerna för Informationssäkerhet och dataskydd gäller för all informationshantering i Region Halland. Därutöver omfattas även bolag, stiftelser och externa leverantörer.

Detta arbete genomförs i enlighet med förvaltningarnas ledningssystem för informationssäkerhet som är framtaget med stöd av standarden för informationssäkerhet, ISO/IEC 27001 och utifrån organisationens verksamhetskrav samt gällande dataskyddslagstiftning och föreskrifter.

Ledningssystemen består av styrande dokument som på övergripande nivå utgörs av policy, riktlinjer och grunddokument och allt informationssäkerhetsarbete utgår från dessa dokument.

Ledningssystemen innehåller även de nödvändiga processer och rutiner som behövs för att säkerställa att all verksamhet uppfyller kraven på informationssäkerhet och dataskydd. Styrande dokument på lokal nivå tas endast fram om det finns ett särskilt behov och ska utformas utifrån regional styrning.

Mål
Säkerhetspolicyns övergripande mål, nedbrutna och förtydligade för respektive område.

- **Information**
  Region Hallands information ska hanteras säkert och skyddas mot de risker som förekommer. Det innebär att skyddet av information, oavsett i vilken form den förekommer, ska anpassas efter skyddsvärdet och de ständigt förändrade hoten och sårbarheterna.

- **Chefer**
  Chefer ansvarar för att bidra till ett effektivt dataskyddsarbete, såväl inom som över förvaltningsgränserna genom att vara säkerhetsmedvetna, ha god kännedom och kunskaper om de risker som finns**.**

- **Medarbetare**
  Region Hallands medarbetare ska vara säkerhetsmedvetna och ha god kännedom och kunskaper om de risker som finns och hur man ska skydda sig mot dem. Medarbetare ansvarar för att följa fastställda regler och rutiner samt vara uppmärksamma på och omgående rapportera avvikelser och misstänkta incidenter.

- **Process**
  Informationssäkerhets- och dataskyddsarbetet ska bedrivas systematiskt och vara en naturlig del i verksamhetens processer där det finns skyddsvärd information. Region Halland ska upprätthålla ett gott skydd för personuppgifter genom att bedriva ett strukturerat dataskyddsarbete i enlighet med fastställda rutiner. Gällande författningar utgör en mininivå för det dataskydd som ska finnas.

- **Teknik**
  Teknisk infrastruktur och system ska vara robusta och säkra. De ska uppfylla verksamhetens krav, lagkrav och skapa verksamhetsnytta. Detta inkluderar även tjänster som Region Halland köper.

- **Integritet**
  Informationssäkerhets- och dataskyddsarbetet ska vara förenligt med medarbetares, patienters och andra registrerades rätt till integritet.

Indikatorer
Indikatorerna ska vara mätbara, uppföljningsbara och ge information om måluppfyllelse.

- **Information**
  - Riskanalyser är genomförda för de delar av infrastrukturen som stödjer Region Hallands verksamhet.
  - Införa system för automatiserad logganalys för system som innehåller känsliga personuppgifter, där det är tekniskt möjligt.

- **Chefer**
  - Medarbetare får tid och utrymme att kontinuerligt delta i utbildningar avseende informationssäkerhet och dataskydd.
  - Uppföljning av genomförda utbildningsinsatser sker löpande.
  - Ansvarar för att vidta nödvändiga åtgärder i samband med rapporterade avvikelser och misstänkta incidenter.

- **Medarbetare**
  - Nyanställda ska genomgå utbildning i informationssäkerhet och dataskydd inom en månad från anställningens början.
  - Kontinuerliga utbildningar i informationssäkerhet och dataskydd ska införas.
  - Medarbetare ska utbildas i incidentrapportering avseende informationssäkerhet och dataskydd.

- **Process**
  - Varje förvaltning har en utsedd informationssäkerhetssamordnare.
  - Varje förvaltning har en utsedd dataskyddssamordnare.
  - Informationssäkerhets- och dataskyddssamordnarna ska ha den ställning som krävs för att arbetet kan prioriteras och utföras effektivt.
  - Upphandlingsprocesserna har kompletterats med krav avseende informationssäkerhet och personuppgiftsbehandling.
  - Det ska finnas strukturerade processer för tilldelning av behörighet och åtkomst till information.
  - Revidering av behörigheter ska ske återkommande.
  - Identitets- och behörighetshantering är automatiserat och centraliserad i hög grad.
  - Det finns en process för att hantera informationssäkerhets- och personuppgiftsincidenter.
  - Det ska snabbt gå att få en överblick över inträffade informationssäkerhets- och personuppgiftsincidenter och avvikelser samt de åtgärder som vidtagits med anledning av dem.
  - Avtal som tecknas med externa leverantörer ska innehålla rutiner för hur leverantören ska klassificera, hantera, kommunicera och samarbeta med Region Halland kring informationssäkerhetsincidenter.

- **Teknik**
  - Endast godkänd programvara ska vara exekverbar (möjlig att öppna/köra) på enheter som ska kunna hantera information som omfattas av sekretess eller som i övrigt är skyddsvärd
  - Det ska finnas fördefinierade skyddsåtgärder för it-säkerhet som är kopplat till informationsklassificeringen.
  - Det ska finnas fördefinierade skyddsåtgärder även för andra områden än it-säkerhet som t.ex. skalskydd och brandskydd.

    - Verktyg används för att upptäcka, undersöka och förhindra att anställda obehörigen röjer mycket känslig information till utomstående i strid med lag, anställningsavtal och policyer.

- **Integritet**
    - Principerna om Privacy by design och Privacy by default ska iakttagas.
    - I den mån det är möjligt, begränsa, pseudonymisera eller avidentifiera personuppgifter som förekommer i logguppgifter.
    - Den information som ges till de registrerade om behandling av personuppgifter, ska leva upp till Dataskyddsförordningens (GDPR) informationskrav.

Genomförande
Genomförandet tar sin utgångspunkt i säkerhetspolicyns övergripande mål som konkretiserats i riktlinjerna. Verksamheten ska styras mot målen.

Förvaltningschefen har ansvaret för att uppfylla målen i sin verksamhet. Säkerhetsarbetet ska vara en del i förvaltningens verksamhetsplan.

Regionkontoret ska vara normerande och stödja förvaltningschefen i planering, genomförande och uppföljning så att målen uppnås. Regionkontoret ska stödja på såväl strategisk som operativ nivå och bidra till utveckling. Tillsammans med förvaltningarna medverka till att skapa helhetssyn genom regiongemensamma tekniska lösningar, stödsystem, rutiner och inriktningar, i syfte att underlätta för verksamheterna att nå målen.

Säkerhetsarbetet hanteras på strategisk nivå i LGV (förvaltningschefer inom hälso- och sjukvård) förstärkt med förvaltningschef Kultur och skola och i viss mån RLG. På operativ nivå i Nätverket för informationssäkerhet.

Uppföljning
- Uppföljning sker i uppföljningsrapport 1, 2, patientsäkerhetsberättelse och årsredovisning.
- Dataskyddsarbetet ska följas upp med regelbundna och systematiska interna revisioner.
- Konsekvensbedömningar avseende dataskydd ska regelbundet redovisas.

Tillhörande dokument:
- Grunddokument: 309 Informationssäkerhet
- Grunddokument: 107 Information, informationsklassning och säkerhetsnivåer
- Rutin: Nätverk informationssäkerhet – uppdrag