Stockholms läns sjukvårdsområde
Närsjukvårdsdirektören

ANMÄLAN
2026-03-05

SLSO 2026-1305

Årsrapport informationssäkerhet för verksamhetsåret 2025

Årsrapport informationssäkerhet för verksamhetsåret 2025 överlämnas till nämnden för Stockholms läns sjukvårdsområde för kännedom.

Stockholms läns sjukvårdsområde

Årsrapport
2026-03-09

Diarienummer
SLSO 2026–1305

Årsrapport

Informationssäkerhet för verksamhetsåret 2025

Innehållsförteckning

Inledning **3**

1. Informationssäkerhetssamordnarens arbete **4**

1.1. Bedömning av resurser 4

2. Ett systematiskt och riskbaserat informationssäkerhetsarbete **4**

3. IT/Informationssäkerhetprojektet **6**

4. Dataskyddsorganisation **6**

5. Incidenter **7**

6. Konklusion **7**

Inledning

Information utgör en av SLSO:s mest betydande tillgångar och är en grundläggande förutsättning för en säker och effektiv verksamhet samt för framsteg inom digitaliseringen. Informationssäkerhet innebär att skydda informationen på ett säkert sätt, oavsett om den är lagrad på papper, digitalt eller muntligt.

Inom ramen för Region Stockholms övergripande ledningssystem för informationssäkerhet är det SLSO:s ansvar att styra och leda sitt informationssäkerhetsarbete genom ett ledningssystem inom sitt verksamhetsområde. Det lokala ledningssystemet ska säkra ett systematiskt informationssäkerhetsarbete och upprätthålla en riskavvägd skyddsnivå i verksamheten. Detta system är en integrerad del av nämndens eller bolagets ordinarie ledningsarbete. Region Stockholms riktlinje för informationssäkerhet och dataskydd Konkretiserar Region Stockholms policy för verksamhetsskydd.

1. Informationssäkerhetssamordnarens arbete

Året har präglats av förändringar inom området, vilket har haft en direkt påverkan på både kontinuitet och styrning. I augusti tillträdde en ny informationssäkerhetssamordnare efter att den tidigare samordnaren avslutat sin anställning i maj. Under perioden däremellan saknades därmed en funktion som kunde hantera de frågor som uppstod i verksamheten.

Eftersom någon parallell överlämning med den avgående samordnaren heller inte kunde genomfördas uppstod dessutom ett glapp i kunskaps- och informationsöverföringen. Detta påverkade under en period möjligheten att upprätthålla en stabil och sammanhållen informationssäkerhetsprocess. Detta påverkar även denna rapport, då informationssäkerhetssamordnaren endast var med en del av året.

1.1. Bedömning av resurser

Rollen som informationssäkerhetssamordnare består av en person som till viss del även är dataskyddsombud. Rollen är beroende av att de stödsystem som används är adekvata och fungerar.

Under hösten och våren har Regions Stockholm infört ett system för hantering av informationstillgångar, IRIS. Införandet har av olika skäl dragits ut på tiden, men bedöms i nuläget att det i stort sett genomfört till slutet av mars 2026 då riskbedömningar åter kan göras i systemet.

Det uppkomna glappet mellan avvecklingen av det tidigare systemet (Complianceportalen) och införandet av det nya systemet (IRIS), som tillhandahålls av Region Stockholm, har medfört en brist i den systematiska kontrollen av både system och verksamheter

Denna avvikelse kommer att hanteras av informationssäkerhetssamordnaren i samverkan med Regionsledningskontoret.

2. Ett systematiskt och riskbaserat informationssäkerhetsarbete

Den 15 januari 2026 trädde cybersäkerhetslagen (2025:1506) i kraft. Lagen utgör Sveriges genomförande av EU:s NIS2-direktiv.

Cybersäkerhetslagen innebär att både offentliga och privata verksamhetsutövare inom vissa samhällsviktiga sektorer är skyldiga att vidta lämpliga åtgärder för att skydda sina nätverks- och informationssystem samt att rapportera betydande incidenter.

Samma datum trädde även en ny riktlinje för informationssäkerhet och dataskydd (RS 2025–0418) i kraft inom Region Stockholm, vilken beaktar den nya lagstiftningen.

Cybersäkerhetslagen ställer krav på nio riskhanteringsåtgärder, som finns reglerade i Region Stockholms styrande dokument.

- Incidenthantering (kap. 13)
- Kontinuitetshantering (kap. 14)
- Säkerhet i leveranskedjan (kap. 12)
- Säkerhetvid förvärv (Kap. 9,11,12)
- Kryptografi (Kap. 7)
- Personalsäkerhet (kap. 4)
- Åtkomstkontroll och förvaltning (kap. 5,6)
- Säkrade kommunikationslösningar (kap. 10)
- Autentisering (kap 6.1)

Mot bakgrund av den nya cybersäkerhetslagen behöver gemensamma processer etableras för förteckning av IT-system, riskhantering samt hantering och rapportering av avvikelser. För att möjliggöra och stödja dessa processer införs därför det regiongemensamma systemstödet IRIS.

En förändring som följer av den nya lagen är att SLSO, från och med lagens ikraftträdande, inte längre omfattas av klassificeringen som anmälningspliktig organisation för samhällskritiska tjänster. Med införandet av NIS2 blir i stället Region Stockholm den ansvariga rapporterande myndigheten. Därmed ska samtliga informationssäkerhetsincidenter rapporteras till Serviceförvaltningen.

3. IT/Informationssäkerhetprojektet

IT- och informationssäkerhetsprojektet, som har bedrivits sedan 2024, befinner sig nu i en utrullningsfas och kommer att utgöra en grund för en mer systematisk uppföljning av de system och tjänster som SLSO ansvarar för. Genom att konsolidera likartade system skapas bättre förutsättningar för ett gemensamt arbetssätt samt en effektiv och samordnad förvaltning.

Införandet av gemensamma systemstöd och arbetssätt bidrar även till att stärka organisationens förmåga att uppfylla kraven i cybersäkerhetslagen. Genom en samlad överblick över IT-system, strukturerad riskhantering samt tydliga processer för incident- och avvikelsehantering skapas bättre förutsättningar för att identifiera, förebygga och hantera cybersäkerhetsrisker i verksamheten.

Vidare ser informationssäkerhetssamordnaren att de processer som införts och förändrats när det gäller införande av nya system, tjänster samt hantering av så kallad skugg-IT (Ej godkända system och tjänster) ytterligare har förändrat förståelsen för den informationen SLSO hanterar till det bättre.

4. Dataskyddsorganisation

I årsrapporten för informationssäkerhet 2024 uppmärksammades behovet av att utveckla arbetet med verksamhetens dataskyddskoordinatorer. Någon förbättring har dock ännu inte kunnat konstateras. Nedan följer en återgivning av vad som framfördes i rapporten.

För att stödja och förbättra det systematiska arbetet med informationssäkerhet och dataskydd har dataskyddskoordinatorer utsetts på verksamhetsområdesnivå och inom de centrala verksamhetsstöden. Denna struktur täcker inte i nuläget hela SLSO och informationssäkerhetssamordnaren ser utmaningar i försöken att inkludera de stora verksamhetsområdena på grund av dess geografiska spridning, organisatoriska storlek och det faktum att varje enhet/verksamhet drivs relativt oberoende av andra enheter/verksamheter. Tillsammans med informationssäkerhetssamordnaren och dataskyddsombudet (DSO) är avsikten att dessa koordinatorer ska hjälpa till att samordna arbetet med informationssäkerhet och dataskydd inom sina specifika verksamhetsområdena och den centrala verksamhetsstöden.

Under verksamhetsåret 2025 har fokus huvudsakligen legat på att höja kunskapsnivån inom gruppen. Eftersom koordinatorerna inte officiellt har

utsetts att arbeta med informationssäkerhet och dataskydd, har informationssäkerhetssamordnaren observerat att det kommer bli utmanande att påbörja operativa åtgärder bland deltagarna i gruppen.

Förslag till åtgärd

Arbetet kommer att fortsätta där informationssäkerhetssamordnare och DSO enligt organisationen ska bli tydligare i sin förväntansbild när det gäller operativa åtgärder. Det kan inkludera att säkerställa genomförandegraden för de obligatoriska utbildningarna.

5. Incidenter

Under 2025 har SLSO varit förskonade från allvarliga informationssäkerhetsincidenter. Inga av NIS-direktivet anmälningspliktiga informationssäkerhetshändelser har inträffat under året.

6. Konklusion

Informationssäkerhetssamordnaren bedömer att SLSO:s arbete med det systematiska och riskbaserade informationssäkerhetsarbetet håller en tillfredsställande nivå, men att det finns utrymme för ytterligare förbättringar. Införandet av verktyget IRIS för informationshantering – innefattande systemförteckning, VIR, personuppgiftsbehandling samt AI-förteckning – förväntas medföra betydande förbättringar i uppföljningsarbetet och stärka den övergripande informationssäkerheten med utökade rapporteringsfunktioner och ökade möjligheter att samarbeta med övriga förvaltningar i Region Stockholm.

Stockholm, mars 2026

John Jacobson

Informationssäkerhetssamordnare