Västerbottens läns landsting
Hälso- och sjukvårdsnämnden

2018-03-27 VLL 2286-2017

2017-11-09 REV 26:3-2017

Landstingets revisorer

Granskning av IT-systemens robusthet

Revisionen har granskat landstingets IT-systems robusthet. Revisorerna lämnade med anledning av granskningen följande rekommendationer till landstingsstyrelsen och hälso- och sjukvårdsnämnden:

- Att fullmäktige tar ställning till ett förslag på informationssäkerhetspolicy för landstinget. Förslaget till policyn bör bland annat inkludera styrelser och nämnders ansvar för informationssäkerhet, inriktning och övergripande mål för informationssäkerhet samt struktur för riskbedömning och riskhantering.
- Att det på landstings- och nämndövergripande nivå och bland verksamheterna finns riskanalyser för informationssäkerhetsområdet.
- Att riktlinjer och regler för informationssäkerhet är väl kända bland berörda medarbetare i landstinget.
- En tillräcklig uppföljning av informationssäkerhetsarbetet inom sina ansvarsområden.

Att tidigare lämnade rekommendationer blir genomförda. Exempelvis:

- Att det genomförs regelbundna kontroller av anställdas behörigheter.
- Att det fattas beslut om vilken prioritetsordning som ska gälla vid återstart i händelse av avbrott i IT-systemen.
- Att det finns en förteckning över landstingets samtliga informationssystem där det framgår vilka av dessa som är att betrakta som kritiska för verksamheten.
- Att det finns beslut om vilka kriterier landstingets serverhallar ska uppfylla avseende fysisk säkerhet, men även att säkerheten i de befintliga hallarna höjs till dess att andra lokaler finns tillgängliga.
- Att beslut om längsta acceptabla tid som informationssystem kan vara ur funktion fattas för alla verksamhetskritiska system.
- Att kontroller av programändringar i IT-systemen genomförs.
- Att periodiska kontroller av användare med access till servrar och databaser genomförs.
- Att det görs kontroller av inloggning till och aktivitet i servrar och databaser.
- Att det genomförs penetrationstester.
- Att landstingets personuppgiftsombud och informationssäkerhetsstrateg har dokumenterade uppdragsbeskrivningar.

Med hänvisning till rekommendationerna i rapporten lämnar landstingsstyrelsen och hälso- och sjukvårdsnämnden följande yttrande:

Nämnden har tagit del av revisionens synpunkter och rekommendationer och instämmer i de synpunkter revisionen framför. Nämnden menar dock att flera aktiviteter och kontroller redan genomförs inom verksamheten för att säkerställa IT-säkerheten. Landstinget har under 2017 initierat och genomfört ett antal åtgärder för att förbättra och säkerställa informationssäkerheten.

Fullmäktiges policyområden består i dag av "Ekonomi och förvaltning", "Kvalitet och säkerhet", "Arbetsmiljö", "Kommunikation", "Miljö", "Jämlikhet och jämställdhet". Det pågår utredning om det är mer lämpligt att uppdatera dessa befintliga policydokument med avsnitt om informationssäkerhet eller om en helt egen policy ska tas fram.

Västerbottens läns landsting
Landstingshuset, Köksvägen 11, 901 89 Umeå
Telefon: 090-785 00 00, telefax: 090-13 68 82
E-post: landstinget@vll.se Org.nr: 232100-0222
VAT-nr: SE232100022201 Bankgiro 5728-3061

Västerbottens läns landsting

2018-03-27

Ett dokument med instruktion för informationsklassning och riskbedömning som utgår från Sveriges Kommuner och Landstings samt Myndigheten för samhällsskydd och beredskaps rekommendationer har under hösten 2017 tagits fram och används löpande i analyser av landstingets olika verksamheters informationsprocesser.

Riktlinjer för informationssäkerhet finns publicerade i landstingets ledningssystem Lita. Riktlinjerna för informationssäkerhet, som anger förhållningssätt vid förvaltning och drift av system samt vid användning av information, är under revidering och kommer att kompletteras med viktiga områden som saknats samt med tydligare struktur på innehållet.

En styrmodell för systematiskt informationsarbete är framtagen. Modellen är ett kvalitetssystem där olika cykliska aktiviteter genomförs och där aktiviteten uppföljning bland annat sker i form av enkät för egenkontroll av informationssäkerhetsarbete.

Landstinget saknar en officiell komplett förteckning över informationssystemen, dock finns en systemdokumentation på IT-system. Det är också gjort en inventering inom enheten för E-hälsa för att dokumentera samtliga IT-system och dess relationer.

Revisionen har i sin granskning konstaterat att det för samtliga av landstingets verksamhetskritiska system inte finns någon informationsklassning och beslut om längsta acceptabla tid som systemen kan vara ur funktion. Det finns dock en beslutad ordning för återstart av systemen i händelse av totalt avbrott och då större delen av systemen ligger nere.

En enklare riskanalys görs årligen i samband med budgetprocessen. Riskanalyser genomförs också vid planerade förändringar i IT-infrastrukturen.

Revisionen har noterat att det saknas kriterier för serverhallarna samt kontroller för tillträde till dessa. Detta kommer att lösa genom att hänvisa till standard. Periodiska kontroller av logglistan görs årsvis. Accesslistan kontrolleras kvartalsvis. Penetrationstester planeras att genomföras under 2018.

Mot bakgrund av revisionens rekommendationer och iakttagelser kommer en åtgärdsplan för att säkerställa IT-systemens säkerhet och robusthet tas fram.

VÄSTERBOTTENS LÄNS LANDSTING
Hälso- och sjukvårdsnämnden

Karin Lundström
Ordförande

Ann-Christin Sundberg
Hälso- och sjukvårdsdirektör