

Granskning av IT-systemens robusthet

Uppföljande granskning

Landstingets revisorer har i flera tidigare granskningar uppmärksammat brister i kontrollen av landstingets IT- och informations-säkerhet. Denna uppföljande granskning visar att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte har vidtagit tillräckliga åtgärder med anledning av revisorernas rekommendationer. Endast fyra av 20 lämnade rekommendationer har blivit helt genomförda.

En slutsats av granskningen är att varken landstingsstyrelsen eller hälso- och sjukvårdsnämnden har säkerställt en tillräcklig styrning, uppföljning och kontroll av IT- och informationssäkerheten inom deras ansvarsområden.

- Det saknas en informationssäkerhetspolicy i landstinget.
- Det saknas landstings- och nämndsövergripande riskanalyser inom informationssäkerhetsområdet.
- Regler och riktlinjer om informationssäkerhet har inte kommunicerats till berörda medarbetare.
- Det saknas uppföljning av att regler och riktlinjer om informationssäkerhet följs.

Rekommendationer

Med anledning av granskningens iakttagelser rekommenderar revisorerna landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa:

- Att fullmäktige får ta ställning till ett förslag på informationssäkerhetspolicy för landstinget.
- Att det på landstings- och nämndsövergripande nivå och bland verksamheterna finns riskanalyser för informationssäkerhetsområdet.

- Att regler och riktlinjer 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 genomförts regelbundna kontroller av anställdas behörigheter, att det fattas beslut om prioriteringsordning vid återstart i händelse av avbrott i IT-systemen, att det finns en förteckning över landstingets samtliga informationssystem där det framgår vilka som är verksamhetskritiska och att det finns beslut om vilka kriterier landstingets serverhallar ska uppfylla avseende fysisk säkerhet samt att säkerheten i befintliga hallar höjs till dess att andra lokaler finns tillgängliga.
- Att övriga i granskningen uppmärksamade brister blir åtgärdade. Exempelvis att beslut om längsta acceptabla tid som informationssystem kan vara ur funktion fattas för alla verksamhetskritiska system, att kontroller av programförändringar i IT-system 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 och att landstingets personuppgiftsombud och informationssäkerhetsstrateg har dokumenterade uppdragsbeskrivningar.

Rapport: "Granskning av IT-systemens robusthet".
För ytterligare information kontakta Eva Röste Moe,
tel. 090-785 73 55. Den kompletta rapporten finns
på landstingets hemsida www.vll.se men kan även
beställas från landstingets revisionskontor.