# 12 UPPFÖLJNING

## 12.1 Mål

*Informationssäkerheten ska, som en del av den ordinarie verksamhetsredovisningen, regelbundet följas upp på central nivå och inom respektive nämnd, styrelse och bolag.*

## 12.2 Utgångspunkt

Enligt regionens Säkerhetspolicy ska säkerhetsarbetet regelbundet följas upp. Detta gäller även informationssäkerhetsarbetet.

Denna uppföljning utgör ett underlag till den övergripande säkerhetsredovisningen som nämnder, styrelser och bolag årligen lämnar till regionstyrelsen.

## 12.3 Uppföljning av efterlevnad

Funktion för informationssäkerheten inom en förvaltning eller ett bolag ska kontinuerligt följa upp informationssäkerhetsarbetet och säkerställa att informationssäkerhet ingår som ett område i styrelsens årliga säkerhetsredovisning och verksamhetens interna kontroll.

Koncernsäkerhetschefen ansvarar på uppdrag av regiondirektören för sammanställning och analys till regionstyrelsen av förvaltningar och bolags säkerhetsredovisning. Koncernsäkerhetschefen kan dessutom vid behov initiera oberoende granskning av informationssäkerheten inom regionen.

### 12.3.1 Personuppgiftsombudets granskningar

Skyddet för den personliga integriteten och efterlevnad av personuppgiftslagen och patientdatalagen granskas särskilt av personuppgiftsombudet.

Personuppgiftsombudet är också den enskildes kontaktyta för att få registerutdrag och hjälp för att få uppgifter rättade eller raderade.

### 12.3.2 Revision av IT-säkerhet

En årlig revision avseende den tekniska säkerheten för infrastrukturen och IT-driften ska göras av VGR IT. I de fall då driften finns hos extern leverantör, ska det i avtalet finnas inskrivet krav på motsvarande revision med VGR IT som mottagare.
Denna revision utgör ett underlag som lämnas in till den övergripande säkerhetsredovisningen till regionstyrelsen.

### 12.3.3 Informations- och resursägarens uppföljning

Inom regionens styr- och förvaltningsmodell för IS/IT följs även informationssäkerhetsarbetet upp som en integrerad del i den ordinarie uppföljningen. Särskild uppmärksamhet ägnas åt att följa upp att ledningssystemet fungerar och att de aktiviteter som beskrivs i ledningssystemet genomförs.

### 12.3.4 Vårdgivarens uppföljning

Enligt Socialstyrelsens föreskrifter om informationshantering och journalhantering i hälso- och sjukvården, SOSFS 2008:14, ställs särskilda krav på att informationssäkerhetsarbetet redovisas till vårdgivaren. I säkerhetspolicy för Västra Götalandsregionen fastställs att regionstyrelsen företräder Västra Götalandsregionen som vårdgivare enligt kraven i patientdatalagen och Socialstyrelsens föreskrifter.

Redovisningen ska omfatta:

- granskningar och skyddsåtgärder av större betydelse som har gjorts i enlighet med Säkerhetspolicyn
- riskanalyser som har utförts avseende informationssäkerheten, och
- vidtagna förbättringsåtgärder

Koncernsäkerhetschefen ansvarar för sammanställning och analys. Rapporteringen utgör ett särskilt område i den årliga säkerhetsredovisningen samt patientsäkerhetsberättelsen.