

## **2 ORGANISATION AV INFORMATIONSSÄKERHETS- ARBETET**

### **2.1 Mål**

*Organisationen ska ha ett högt riskmedvetande och informationssäkerhetsarbetet ska vara organiserat, så att det finns ett tydligt ansvar och väl fungerande beredningsprocesser.*

### **2.2 Utgångspunkt**

Ansvar för informationssäkerhet följer ordinarie linjeansvar, vilket innebär att även informationsägarskapet följer linjeansvaret. Inom VGR:s styr- och förvaltningsmodell för IS/IT företäder objektägare verksamhet informationsägaren.

Regelverkets krav på VGR IT och dess chef gäller i motsvarande grad andra organisationer inom VGR som bedriver IT-drift och utveckling, exempelvis Västtrafik

Informationssäkerhetsfrågor ska vara en integrerad del i berednings- och inköpsprocessen för IS/IT.

### **2.3 Samordning och uppföljning**

Koncernsäkerhetschefen leder ett informationssäkerhetsråd, för samordning och uppföljning av regionens informationssäkerhetsfrågor. I rådet ingår sakkunniga med mandat att företräda sin förvaltning och relevanta experter.

Representanter från informationssäkerhetsrådet och personuppgiftsombuden ska delta i IS/IT-beredningen och granska informationssäkerhetsaspekten. Detta gäller såväl på förvaltningsnivå som på regional nivå.

Utöver detta finns ett regionalt riskhanteringsråd, se punkt 4.5.

I kravställning av informationssäkerhet på nationella IS/IT-tjänster, ska denna grundas på verksamheternas behov. Koncernsäkerhetschefen ansvarar för att samordna med övriga länsting och regioner.

### **2.4 Övergripande informationssäkerhetsansvar**

#### ***Regionfullmäktige***

Se Säkerhetspolicy för Västra götalandregionen

#### ***Regionstyrelsen***

Se Säkerhetspolicy för Västra götalandregionen

#### ***Regiondirektör***

Se Säkerhetspolicy för Västra götalandregionen

#### ***Koncernsäkerhetschef***

Enligt Socialstyrelsens föreskrifter ska vårdgivaren utse en eller flera som ansvarar för informationssäkerheten. Detta ingår i koncernsäkerhetschefens uppdrag.

***Personaldirektören***

Ansvarar för att säkerhetskraven införs i personalhanteringsprocessen före, under och efter anställning.

***Fastighetsdirektören***

Ansvarar för att kraven på fysiskt skydd beaktas i byggnadsprocessen.

***IS/IT-direktören***

Ansvarar för att IT-säkerheten (teknisk säkerhet, ansvar och rutiner) motsvarar ställda krav.

***Chef inköpsorganisation***

Ansvarar för att informationsägarens säkerhetskrav beaktas i inköpsprocessen.

## **2.5 Verksamhetsansvar – roller och ansvar på förvaltningsnivå**

***Nämnder, styrelser och bolagsstyrelser***

Se Säkerhetspolicy för Västra götalandregionen

***Förvaltningschef***

Ansvarer för tillämpning av ledningssystemets regelverk i den egna förvaltningen, utforma lokala regelverk och rapportera status på informationssäkerhetsarbetet till nämnd/styrelse. Förvaltningschefen ska avsätta resurser för informationssäkerhetsarbetet och säkerställa att riskhanteringsprocessen blir en del av det lokala ledningssystemet.

***Verksamhetschef/motsvarande***

Ansvarar för informationssäkerhet inom egen verksamhet och ska verka för att arbetsmetoder som bidrar till en god informationssäkerhet används, samt att medarbetarna får utbildning i informationssäkerhet.

***Medarbetare***

Medarbetare ska ha förståelse för värdet av informationen och varför den ska skyddas. Detta innebär att medarbetaren ska få utbildning, som bidrar till en god säkerhetskultur och medvetenhet om det egna ansvaret.

Alla medarbetare har ansvar att följa gällande regler avseende informationssäkerhet.

***Personuppgiftsombud (PuO)***

Har till uppgift att självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed samt genomföra revision.

***Samordnare informationssäkerhet/motsvarande***

Ansvarar för att samordna och följa upp informationssäkerhetsarbetet i den egna verksamheten och rapportera direkt till förvaltningschefen. Hen ska aktivt bidra med kunskap och aktiviteter i samordning och uppföljning av det regiongemensamma informationssäkerhetsarbetet.

***Samordnare IS/IT (SIS)***

Samordnar förvaltningens kravställning på IS/IT och samverkar med samordnaren för informationssäkerhet, så att informationssäkerhetskraven blir en del av förvaltningens samlade kravbild på IS/IT.

## 2.6 Centrala roller

I kravställning och införande av informationssäkerhet i IS/IT-tjänster är informationsägare och resursägare centrala roller. Alla informationstillgångar ska ha en utsedd ägarföreträdare inom Västra Götalandsregionen.

### ***Informationsägare – objektägare verksamhet***

Ansvar som informationsägare följer linjeansvar. Informationsägaren ansvarar för den information som skapas och hanteras inom den egna verksamheten. När information ingår i objekt, enligt regionens styr- och förvaltningsmodell för IS/IT, företräds informationsägaren i tillämpliga delar av objektägare verksamhet.

### ***Resursägare – objektägare IT***

Resursägare är den som äger teknik, infrastruktur eller IS/IT-tjänster. Inom regionens styr- och förvaltningsmodell för IS/IT är objektägare IT resursägare. I övriga fall ska en resursägare utses i respektive förvaltning.

*I fortsättningen används begreppen **informationsägare** och **resursägare** i detta dokument. Kontexten avgör om det är aktuellt inom en förvaltning alternativt inom VGR:s styr- och förvaltningsmodell för IS/IT.*