

1 ÖVERGRIPANDE INFORMATION OM LEDNINGS- SYSTEMET

Riktlinjerna för informationssäkerhet utgår från Säkerhetspolicy för Västra Götalandsregionen.

Enligt policyn är det övergripande målet för informationssäkerheten
”att rätt och riktig information ska nå rätt mottagare i rätt tid och vara skyddad för obehörig åtkomst och förstörelse”.

Informationssäkerhet handlar om att tillgodose krav på:

Tillgänglighet	Möjlighet att utnyttja information efter behov i förväntad utsträckning och inom önskad tid.
Riktighet	Skydd av informationen så att den är och förblir korrekt och fullständig.
Konfidentialitet	Informationen är tillgänglig endast för den som är behörig att ta del av och använda den.
Spårbarhet	Möjlighet att i efterhand visa hur och av vem informationen har hantearats.

Informationssäkerhet är teknikneutral och omfattar skydd av såväl muntlig, pappersbunden som digital information.

1.1 Giltighet

Denna riktlinje är beslutad av regionstyrelsen och utformad med stöd av Säkerhetspolicyn. Den gäller således alla Västra Götalandsregionens förvaltningar och majoritetsägda bolag samt avtalsparter, där det i avtalet anges att regionens regelverk ska följas.

Denna riktlinje ersätter:

- Informationssäkerhetspolicy, RSK 541-2000, beslutad av regiondirektör Jan-Åke Björklund 4 april 2000
- Reglemente för informationssäkerhet, RSK 541-2000, beslutad av regionfullmäktige 7 maj 2002, § 124
- Riktlinjer för informationssäkerhet, RSK 703-2006, beslutade av regionstyrelsen 23 juni 2009, § 150

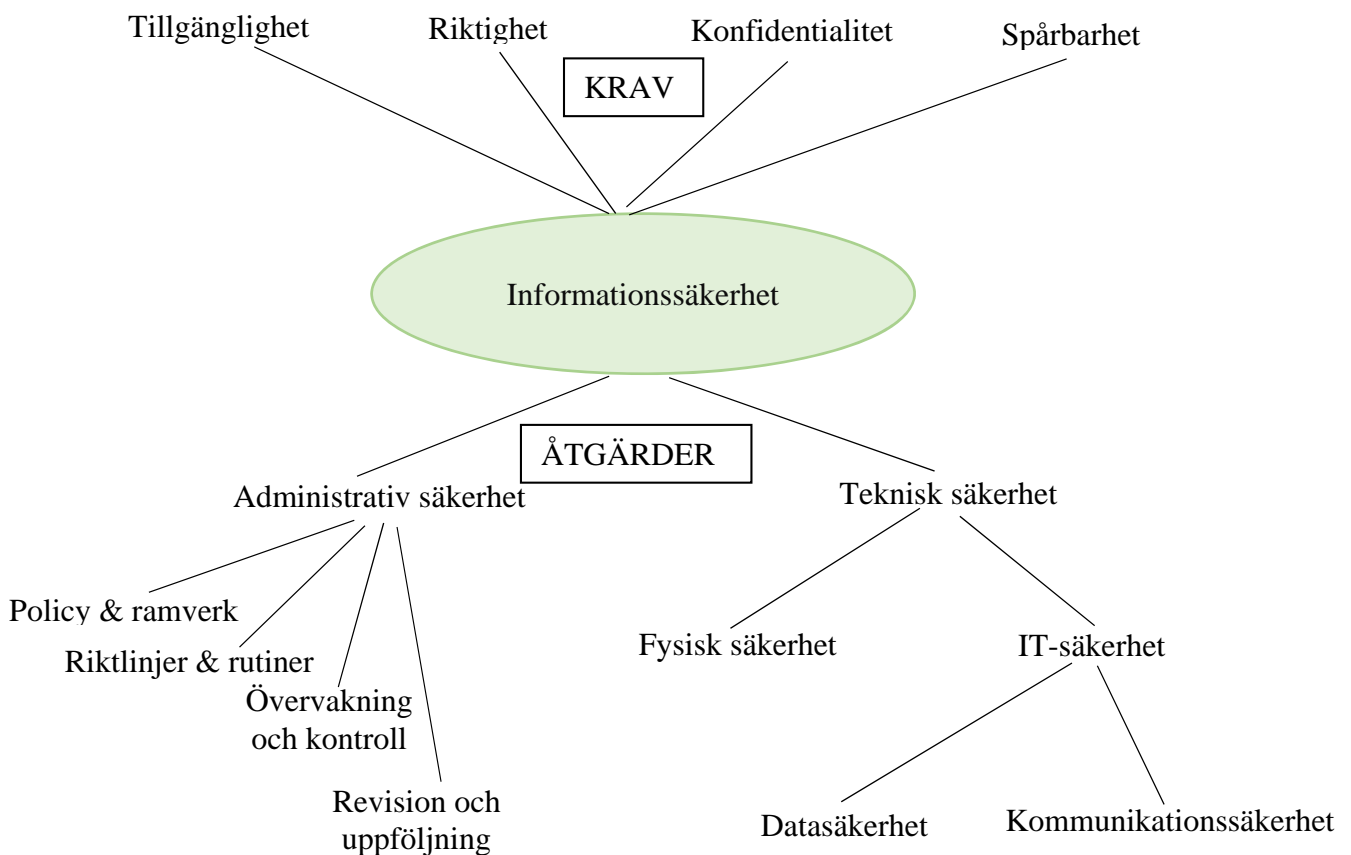
Koncernsäkerhetschefen ansvarar på regiondirektörens uppdrag för förvaltning och förslag till eventuell revidering av riktlinjerna för informationssäkerhet. Med hänsyn till verksamhetens art kan avvikelser från bestämmelserna göras efter samråd med koncernsäkerhetschefen.

1.2 Begreppet informationssäkerhet

Informationssäkerhet kan beskrivas som att tillgodose behov av att informationen är **tillgänglig** i förväntad utsträckning, förblir **riktig** och oförvanskad, är insynsskyddad så att den är åtkomlig endast för den som är behörig – **konfidentialitet** – samt att det finns **spårbarhet** i vem som haft åtkomst till och/eller förändrat informationen. Se de fyra övre begreppen i illustrationen bild 1.

För att uppnå de krav som ställs utifrån de fyra begreppen används olika former av skyddsåtgärder, som tillsammans ska åstadkomma rätt informationssäkerhet. Se nedre delen av illustrationen, bild 1.

Bild 1: Schematisk bild av det som ska skyddas samt skyddsåtgärder



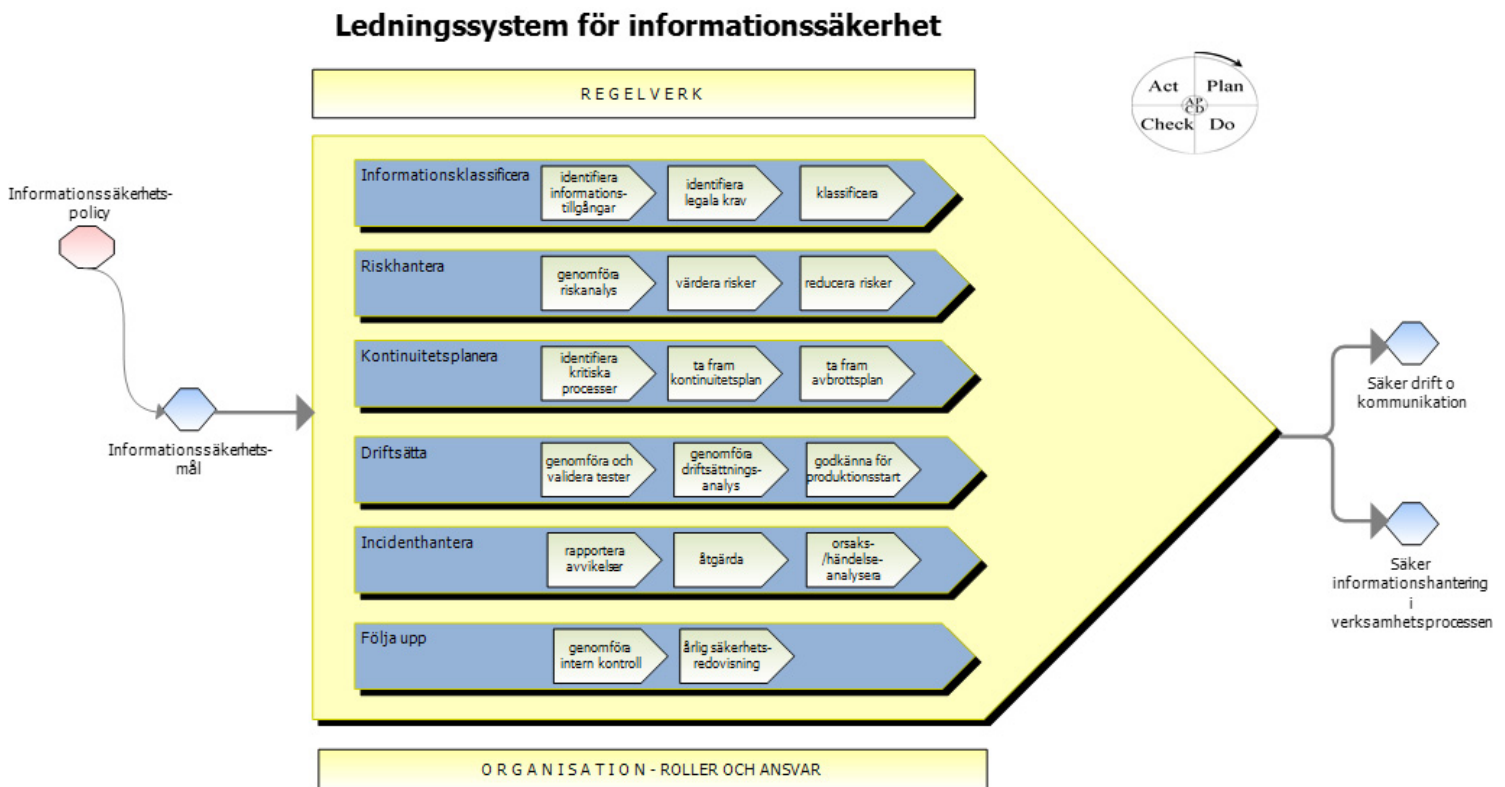
1.3 Styrning, ledning och arbete med informationssäkerhet

För att uppnå en god informationssäkerhet krävs ett långsiktigt arbete, som bygger på ett systematiskt säkerhetsarbete integrerat i det dagliga arbetet. Arbetet ska inkludera alla områden som hanterar informationstillgångar.

Regionledningen styr och följer upp arbetet med stöd av ett system som inkluderar mål, regelverk, organisation och processer.

Inom ramen för Västra Götalandsregionens styr- och förvaltningsmodell för IS/IT ska det genomföras säkerhetsaktiviteter vid beredning/projekt, utveckling, införande, förvaltning och avveckling av informationssystem.

Bild 2: Beskrivning av ledningssystemets komponenter och uppbyggnad



1.4 Dokumentstruktur

Regionala styrdokument i ledningssystemet för informationssäkerhet är policy och riktlinjer som är beslutade på politisk nivå. Till dessa finns VGR-riktlinjer och VGR-rutiner beslutade av koncernsäkerhetschef. Inom ramen för dessa kan objektägare – verksamhet och IT – ta fram och besluta om objektspecifika rutiner. För att säkerställa sammanhållen helhet i ledningssystemet ska dessa kvalitetssäkras av säkerhetsstrategiska enheten före publicering. Dessa regionala styrdokument finns samlat publicerade på intranätet.

Styrande dokumenten på lokal nivå utformas utifrån regionala styrdokument för informationssäkerhet.

Bild 3: Beskrivning av dokumenthierarki för regionens regelverk för informationssäkerhet

