VÄSTRA GÖTALANDSREGIONEN

Koncernkontoret
Säkerhetsenheten

Dokumenttyp	Övergripande dokument	Version
RS-riktlinjer för informationssäkerhet för Västra Götalandsregionen	Säkerhetspolicy för Västra Götalands-regionen	3.0
Dokumentansvarig	Kontaktperson	Dnr
Valter Lindström, koncernsäkerhetschef		RS 1594-2013
Beslutad av	Giltig från	Ersätter
Regionstyrelsen	2015-09-01	Riktlinjer för informationssäkerhet, RSK 703-2006.

RS-riktlinjer för Informationssäkerhet i Västra Götalandsregionen

RS 1594-2013

INNEHÅLLSFÖRTECKNING

Innehåll

1 ÖVERGRIPANDE INFORMATION OM LEDNINGSSYSTEMET

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 hanterats.

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

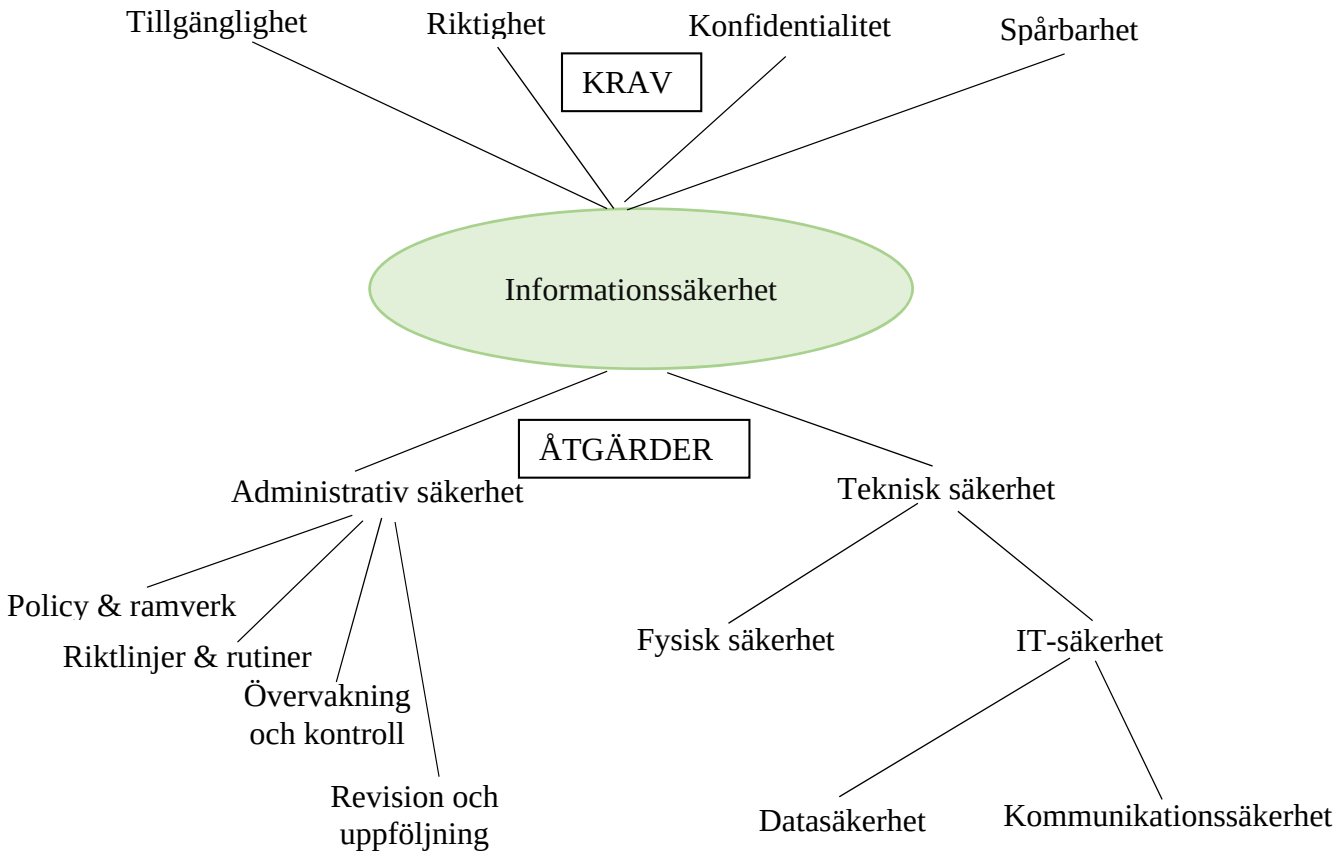
Koncernsäkerhetschefen ansvarar på regiondirektörens uppdrag för förvaltning och förslag till eventuell revidering av riktlinjerna för informationssäkerhet. Med hänsyn till verksamhetens art kan avvikelse från bestämmelserna göras efter samråd med koncernsäkerhetschefen.

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

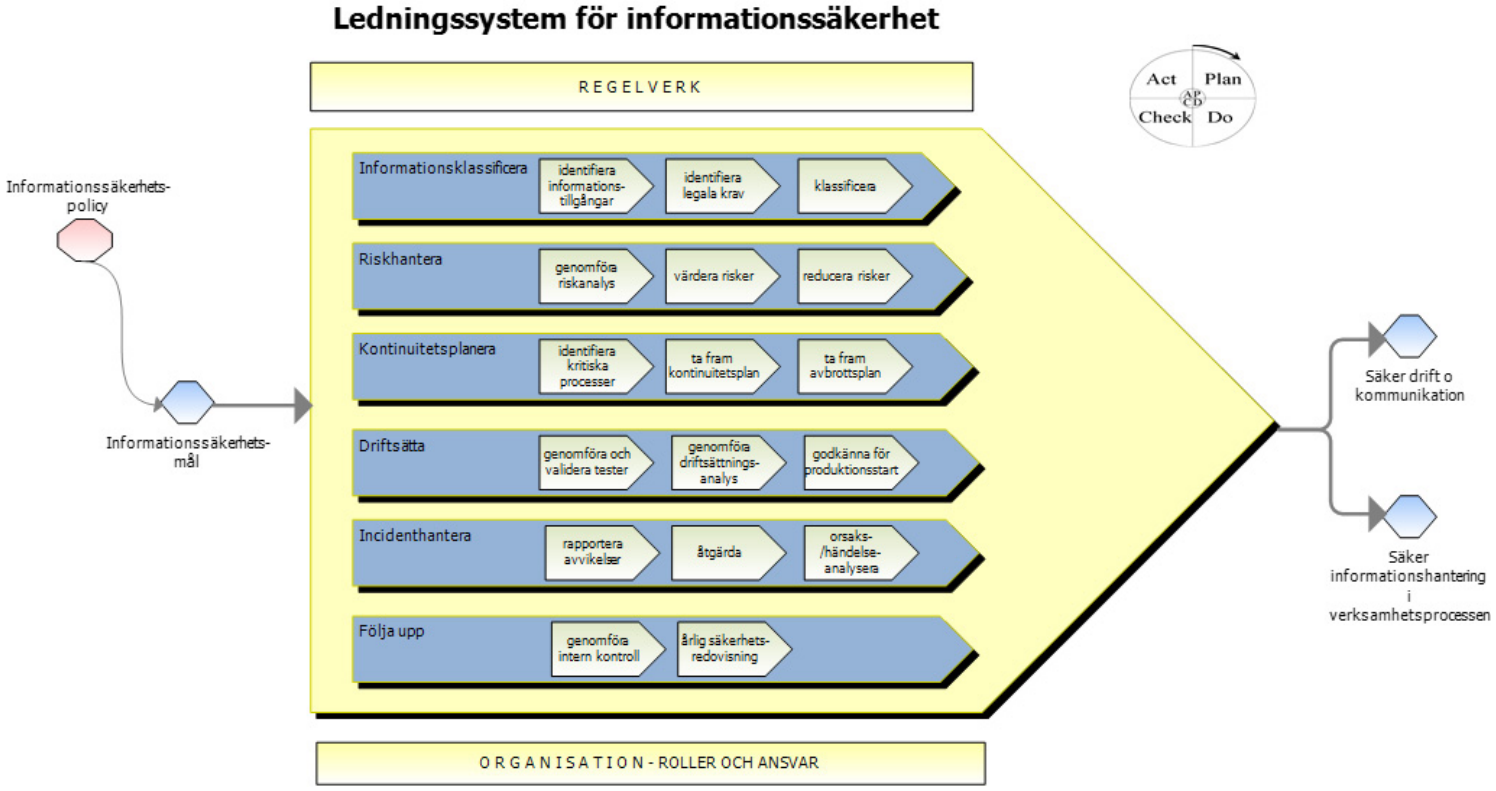


1.3 Styrning, ledning och arbete med informationssäkerhet

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

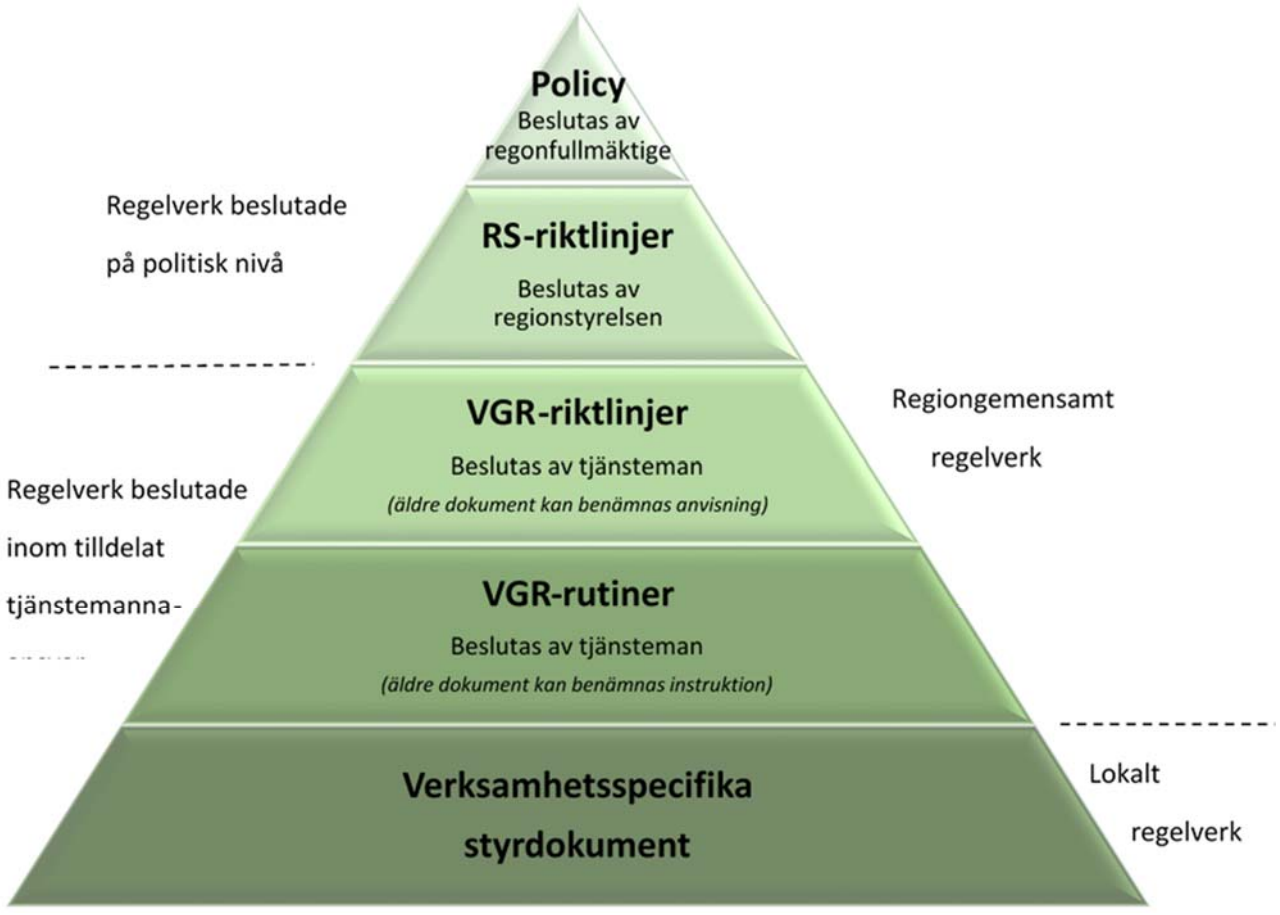


1.4 Dokumentstruktur

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



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 företräder 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 beredning- 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 landsting och regioner.

2.4 Övergripande informationssäkerhetsansvar

Regionfullmäktige
Se Säkerhetspolicy för Västra götalandsregionen

Regionstyrelsen
Se Säkerhetspolicy för Västra götalandsregionen

Regiondirektör
Se Säkerhetspolicy för Västra götalandsregionen

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 götalandsregionen

Förvaltningschef
Ansvaret 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.*

3 STYRNING AV INFORMATIONSTILLGÅNGAR

3.1 Mål

All information och övriga informationstillgångar ska vara kopplade till en ägarföreträdare, som har ansvar för att informationen och resurserna klassificeras och skyddas på rätt sätt.

3.2 Utgångspunkt

Informationssäkerhetsarbetet ska ske utifrån generella säkerhetskrav (Säkerhetspolicy och Riktlinjer för informationssäkerhet) och de specifika säkerhetskrav som ställs av verksamheten genom informationsklassificering.

3.3 Märkning av handlingar

Tryckfrihetsförordningen och Offentlighets- och sekretesslagen (2009:400) styr hur allmänna handlingar ska hanteras i offentlig verksamhet. Allmän handling ska lämnas ut på begäran, under förutsättning att den inte omfattas av sekretess.

I Västra Götalandsregionen används följande begrepp, förutom allmän handling, för handlingar:

- Utkast — Minnesanteckning – bakgrundsmaterial som har tillkommit endast för ärendets beredning eller föredragning, dock inte till den del den tillför ärendet sakuppgift.
- Sekretessbelagd — Handling som är sekretessbelagd med stöd av Offentlighets- och sekretesslagen

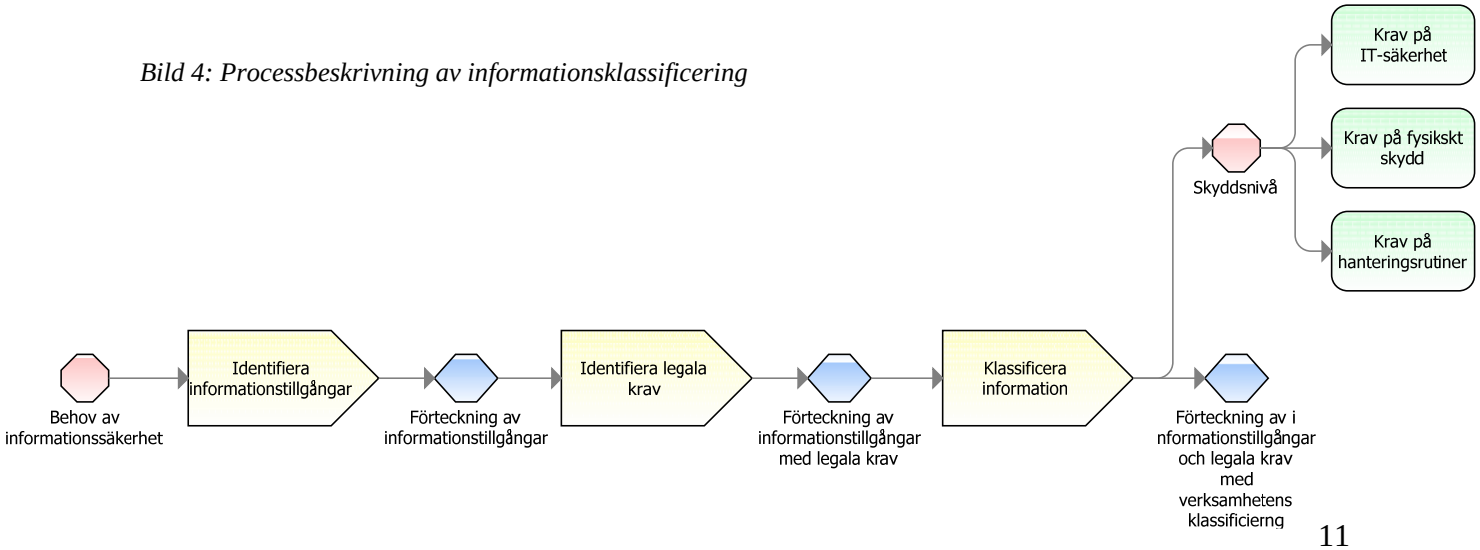
3.4 Informationsklassificering

Informationsägaren ska styra och skydda informationstillgångarna, med utgångspunkt från det värde informationen har för verksamheten. Informationsklassificering är därför en grundläggande aktivitet, för att kravställa skyddsåtgärder och skydda informationen på rätt sätt.

Inom regionens styr- och förvaltningsmodell för IS/IT företräder objektägare verksamhet också informationsägaren och är därmed ansvarig för att informationsklassificering görs ur ett verksamhetsperspektiv och blir en del av objektets dokumentation.

Övriga informationstillgångar, som inte tillhör ett objekt, hanteras inom respektive förvaltning.

Bild 4: Processbeskrivning av informationsklassificering



3.4.1 Identifiera informationstillgångar

Första steget är att identifiera vilken information som hanteras inom avgränsningen för klassificeringen. Utgångspunkten är verksamhetsperspektivet och vilken information som behövs/produceras i verksamhetsprocessen/objektet. Även de resurser som krävs för att hantera informationen identifieras.

3.4.2 Identifiera legala krav

Nästa steg är att identifiera de legala krav som är tillämpliga för hanteringen av informationen och bedöma hur väl de uppfylls. Med legala krav avses lagkrav, föreskrifter och avtal.

3.4.3 Klassificera information

Klassificeringen av informationen bestäms utifrån det värde den har i verksamhetsprocessen och vilka krav på skydd verksamheten ställer utifrån följande begrepp:

- **Tillgänglighet –** möjlighet att utnyttja information efter behov i förväntad utsträckning och inom önskad tid
- **Riktighet** – skydd av information så att den är och förblir korrekt och fullständig
- **Konfidentialitet** – information 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 information har hanterats

Klassificeringen genomförs med stöd av VGR:s metod, se *VGR-rutin för klassificering av informationstillgångar*.

Klassificering ska som ett minimum genomföras/aktualiseras vid:

- Etablering av nya IS/IT-system
- Organisations-/processförändringar som kan påverka informationsbehandlingen
- Tekniska förändringar i infrastruktur eller programvaror, som kan påverka informationsbehandlingen
- Om molntjänster eller outsourcing av funktioner eller IS/IT-tjänst övervägs
- Vid allvarliga händelser/incidenter

3.5 Skyddsnivåer

Informationsklassificeringen ska leda till funktionella säkerhetskrav på tekniken samt hanteringsrutiner i verksamheten, som tillsammans uppfyller en säkerhetsnivå som motsvaras av klassificeringen – rätt säkerhet.

3.5.1 Skyddsnivå i verksamhet

Informationsägaren ansvarar för att det finns tydliga rutiner för hur informationen får hanteras i verksamheten.

Reglerna ska omfatta all behandling av information.

Regler och skyddsåtgärder ska omfatta olika typer av bärare av information som USB-minnen, DVD-skivor, ljudinspelningar, fotografier, telefoner, läsplattor, pappersdokument, m.m.

3.5.2 Skyddsnivå IS/IT-tjänster och fysiskt skydd

Resursägaren ansvarar för att det finns tekniska lösningar och administrativa driftrutiner som motsvarar informationsägarens klassificering.
Resursägaren ansvarar för att skyddsåtgärder regelbundet uppdateras och finns med i avtal med extern leverantör av IS/IT-tjänst.

3.6 Säkerhetsdeklaration

För viss typ av IS/IT-tjänst/-funktion är informationsklassificering inte tillämpbart. Då är det lämpligare att genomföra en säkerhetsdeklaration. Syftet med denna är att deklarera vilken säkerhetsnivå tjänsten/funktionen levererar. Detta utgör ett underlag för styrning av användningen. Se *VGR-rutin för säkerhetsdeklaration.*

Resursägaren och informationsägaren ansvarar för att fastställa säkerhetsdeklarationen och, om så behövs, kommunicera hanteringsrutiner.

4 RISKHANTERING

4.1 Mål

Risker som kan påverka Västra Götalandsregionens informationssäkerhet ska identifieras, analyseras och hanteras.

4.2 Utgångspunkt

Ramverket för säkerhet och perspektiven **före–under–efter** tillämpas såväl för informationssäkerhet som för annat säkerhetsarbete. Tyngdpunkten ligger på det förebyggande arbetet där riskhantering är en grundläggande aktivitet.

Allt säkerhetsarbete utgår från det som är skyddsvärt för VGR och medborgarna.

4.3 Riskhantering

Riskhantering är samordnade aktiviteter för att leda och styra en organisation med avseende på risk. Riskhanteringsprocessen i Västra Götalandsregionen är en generisk modell, som ska tillämpas av varje verksamhet och vara en del av beslutsunderlaget inför förändringar.

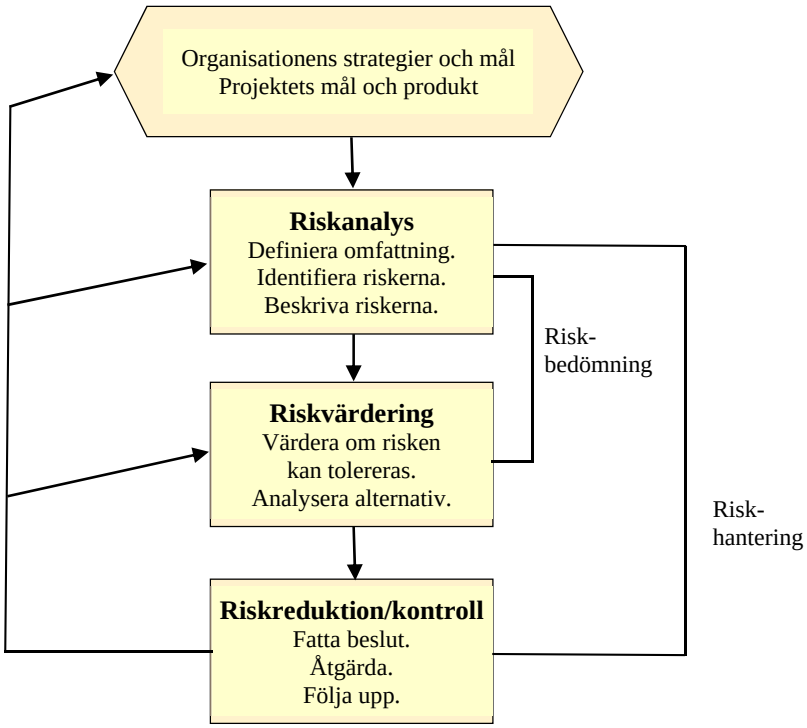


Bild 5: Schematisk bild av riskhantering

För genomförande av riskanalys se *VGR-rutin för riskanalys*.

Riskhantering ska som minimum genomföras vid:

- Etablering av nya IS/IT-system
- Organisations-/processförändringar som kan påverka informationsbehandlingen
- Tekniska förändringar i infrastruktur eller programvaror, som kan påverka informationsbehandlingen
- Om molntjänster eller outsourcing av funktioner eller IS/IT-tjänst övervägs.

4.3.1 Uppföljning

För att kontrollera om effekten är den önskade ska genomförda aktiviteter och fattade beslut dokumenteras och följas upp.

4.4 Ansvar

Ansvaret för riskhanteringen följer linjen, vilket innebär att respektive förvaltning ska integrera riskhanteringsprocessen och dess aktiviteter i det egna ledningssystemet. Det ska tydligt framgå i vilka forum som beslut om åtgärder fattas.

I regionens styr- och förvaltningsmodell för IS/IT ansvarar respektive informations- och resursägare för att riskhanteringsprocessen genomförs, i samverkan med berörda verksamheter. Samma beslutsvägar tillämpas som för övriga objektbeslut.

4.5 Eskalering av hot och risker av regiongemensam karaktär

Hot och risker som inte kan hanteras i linjen eller inom VGR:s styr- och förvaltningsmodell för IS/IT ska eskaleras till koncernsäkerhetschefen, för beredning i det regionala riskhanteringsrådet och därefter beslut av regiondirektör alternativt beslut i lämplig politisk församling.

5 PERSONAL OCH SÄKERHET

5.1 Mål

Alla medarbetare som hanterar regionens informationstillgångar, ska ha kännedom om regionens regelverk och tillräcklig kompetens för att kunna utföra sina arbetsuppgifter på ett säkert sätt.

5.2 Utgångspunkt

När begreppet medarbetare används avses även uppdragstagare och externa leverantörer.

5.3 Före anställning

5.3.1 Rekrytering av medarbetare

Kontroller ska ske i enlighet med *Regionövergripande riktlinjer vid rekrytering*, framtagna av Regionkansliets HR-strategiska avdelning.

Vid rekrytering eller befordran till särskilt informationssäkerhetskritiska arbetsuppgifter, ska flera och mer detaljerade kontroller övervägas.

Det ska i anställnings- eller arbetsvillkor vara tydligt vilken information som ägs av arbetsgivaren och som inte får förstöras, kopieras eller röjas vid t.ex. avslutande av tjänst.

Vid anställning ska informeras om

- Hur och för vad den anställdes personuppgifter registreras
- Regler för datoranvändning
- Att arbetsgivaren kan genomföra kontroll vid misstanke om att den anställde bryter mot gällande regelverk och/eller lagstiftning
- Att kontroll kan ske i lokal pc, mobila enheter, hemmakataloger, e-postsystem loggar m.m.

5.3.2 Sekretess

Inom den offentliga sektorn är sekretess för de anställda reglerat i lag. Sekretessförbindelse är därför inte möjlig att använda, utan ersätts av en påminnelse om sekretess. Anställda ska skriva under att man mottagit påminnelse om sekretess. Anställda kan inte avkrävas någon tystnadsplikt utöver vad som anges i offentlighets- och sekretesslagen (SFS 2009:400) samt yttrandefrihetsgrundlagen (SFS 1991:1469).

Inom sjukvården ska det i påminnelse om sekretess anges, vilka regler som gäller för inre respektive yttre sekretess, för rätten att ta del av eller vidarebefordra patientuppgifter.

Personer som inte har en anställning i Västra Götalandsregionen, exempelvis studerande, konsulter och andra som använder regionens resurser för informationsbehandling, ska också informeras och skriva under sekretessförbindelse.

5.4 Under anställning

5.4.1 Regelbunden utbildning av alla medarbetare

Chef har ansvar för att alla medarbetare får utbildning och information inom området informationssäkerhet, inklusive betydelsen av avvikelserapportering. Vid förändringar och tillägg av informationssäkerhetsregelverket, har varje chef ansvar för att de blir kända av medarbetarna.

5.4.2 Disciplinär process

Vid misstanke om brott mot gällande lagstiftning, ska närmaste chef och HR-avdelningen informeras och polisanmälan upprättas.

Vid misstanke om överträdelse av gällande regelverk inom Västra Götalandsregionen, ska detta hanteras på motsvarande sätt, med undantag för polisanmälan.

5.5 Upphörande eller förändring av anställning

Det ska på förvaltningsnivå finnas rutiner, som är utformade så att en persons tillgång till information och data snabbt anpassas i samband med organisationsförändringar, förändrade arbetsuppgifter eller upphörande av anställning. Se även kapitel 9, Åtkomst till information.

6 FYSISK SÄKERHET

6.1 Mål

Västra Götalandsregionens information samt övriga informationstillgångar, som exempelvis lokaler och den utrustning som används för informationshantering, ska skyddas på en nivå som identifierats genom informationsklassificering.

6.2 Utgångspunkt

Kraven på fysisk säkerhet finns beskrivna i *VGR-riktlinje för fysisk säkerhet* och ska tillämpas för alla lokaler där information hanteras, samt för all utrustning som används för informationshantering. Information och utrustning ska skyddas på ett likvärdigt sätt, oavsett om den hanteras innanför eller utanför regionens lokaler. Utöver ovanstående riktlinje ska Arkivnämndens regler och rekommendationer iakttas för lokaler som förvarar arkivmaterial.

7 UTVECKLING AV IS/IT-TJÄNSTER

7.1 Mål

Informationssäkerhet ska beaktas under hela IS/IT-tjänstens livscykel.

7.2 Utgångspunkt

Vid anskaffning, utveckling, underhåll och avveckling av IS/IT-tjänster ska informationssäkerhetskraven tillgodoses.

Kravställningen tar sin utgångspunkt från gällande regelverk, informationsägarens klassificering och är en del av IS/IT-beredningen.

Kraven på utveckling av IS/IT-tjänster finns beskrivna i *VGR-riktlinje för styrning av utveckling, införande och förvaltning av IS/IT*. Kraven ska även ställas på externa leverantörer som nyttjas vid utveckling, underhåll och avveckling av IS/IT-tjänster.

8 KOMMUNIKATION OCH DRIFT

8.1 Mål

Kommunikation och drift av IS/IT-miljö, system och tillhörande resurser ska ske utifrån fastställda rutiner för gemensam infrastruktur och de specifika säkerhetskrav som ställs av verksamheten genom informationsklassificering.

8.2 Utgångspunkt

VGR:s verksamhet bygger på informationshantering i ett stort antal system, tjänster och resurser. För att få rätt nivå på säkerhet i denna helhet krävs tydlig ansvarsfördelning, eftersom säkerhetskraven från informationsägaren ska tas om hand av olika system- och resursägare.

Det ska finnas en IT-säkerhetsstrategi, som leder till en långsiktig säkerhetsarkitektur för VGR. Arkitekturen ska vara dokumenterad och följa regionens ledningssystem för informationssäkerhet.

IS/IT-direktören ansvarar för att upprätta och förmedla en tjänsteportfölj med säkerhetsteknik, som matchar skyddsnivåerna enligt modellen för informationsklassificering. Skyddsnivåerna ska användas för både interna och externa system- och resursägare.

Kraven på drift och kommunikation finns beskrivna i *VGR-riktlinje för drift och kommunikation* och ska tillämpas i drift och förvaltning av VGR:s informationsbehandlingsresurser. Kraven ska även ställas på externa leverantörer som används för drift, förvaltning och kommunikation.

9 ÅTKOMST TILL INFORMATION

9.1 Mål

Användare ska ha tillgång till rätt information på rätt sätt för sin arbetsuppgift och vara medveten om sitt personliga ansvar.

Lämpliga krav på spårbarhet ska finnas omsatta i all informationshantering, samtidigt som den personliga integriteten värnas.

9.2 Utgångspunkt

Åtkomst till information ska ges enligt klart definierade principer, tydliga ansvarsförhållanden och enhetliga metoder. Det ska finnas ansvar, rutiner och tekniska skyddsåtgärder som styr användares åtkomst till information och IS/IT-tjänster. Detta gäller även för externa IS/IT-tjänster och mobil utrustning.

Informationsklassificering styr vilka krav på identifiering och behörigheter som ska ställas. Se *VGR-rutin för klassificering av informationstillgångar.*

Västra Götalandsregionens grundläggande värderingar bygger på god etik och moral, vilket innebär att det inte är tillåtet att besöka sidor som innehåller pornografiskt material, hot, förtal, våld, terror, rasism, hets mot folkgrupp, mobbning, brott mot diskrimineringslagen eller uppmaning till droganvändning.

Samma begränsning gäller för besökare, patienter, studerande och andra användare som ges tillgång till regionens nät

Kraven för åtkomst till information finns beskrivna i *VGR-riktlinje för åtkomst till information* och ska tillämpas för all hantering av åtkomst till information.

10 HANTERING AV INFORMATIONSSÄKERHETSINCIDENTER

10.1 Mål

Process, organisation och resurser för avvikelse- och incidenthantering ska finnas, för att mildra effekter, förhindra upprepande och underlätta återgång till verksamhet på normal nivå, då någon form av säkerhetsincident inträffat.

10.2 Utgångspunkt

Det ska finnas ansvar och rutiner för rapportering, eskalering och uppföljning av informationssäkerhetsincidenter inom Västra Götalandsregionen och varje förvaltning/bolag. Reglerna berör inte enbart händelser, utan även sårbarheter som kan göra att hot förverkligas till incidenter.

Avvikelser/incidenter med informationssystem som är klassade och CE-märkta som medicinteknisk produkt ska enligt Socialstyrelsens författning SOSFS 2008:1 anmälas till tillverkaren och läkemedelsverket. Allvarliga avvikelser/incidenter med egentillverkade medicinska produkter ska anmälas till inspektionen för vård och omsorg.

En händelse som kan innebära en kris ska eskaleras enligt Regional Krishanteringsplan.

10.3 Medarbetares skyldighet

Det är ett krav att varje medarbetare omgående rapporterar sårbarheter, avvikelser och incidenter inom informationssäkerhetsområdet. Rapportering ska ske till närmaste chef eller till den som av chef utsetts att ta emot dessa anmälningar. Registrering i regionens system för avvikelser ska också ske.

I de fall rapportering till närmaste chef bedöms olämplig, ska rapport om brister i informationssäkerheten lämnas till förvaltningens samordnare för informationssäkerhet eller koncernsäkerhetschef.

10.4 Verksamhetsansvarigs skyldighet

Vid allvarligare händelse ska en händelse-/orsaksanalys genomföras. Även vid mindre allvarliga händelser där det finns ett viktigt lärandeperspektiv bör analys göras. På begäran av verksamheten ska regionens IS/IT-organisation bidra och delta i händelseanalysen.

Vid händelse som gäller personuppgifters riktighet och när den enskildes integritet kan ha kränkts, ska personuppgiftsombudet (PuO) informeras.

10.5 IT-levererande parts skyldighet

IT-levererande part har skyldighet att skapa rutiner och organisation för att hantera IS/IT-incidenter. I rutinen ska ingå att alltid skapa incidentrapport, som ska delges berörda parter.

I syfte att identifiera systematiska fel och åtgärda dessa, ska händelse-/orsaksanalys genomföras. Analys kan initieras av IT-levererande part i samråd med VGR IT, förvaltning eller begäras av drabbad verksamhet.

Även vid händelser av mindre karaktär har IT-levererande part skyldighet att samverka med berörda verksamheter och vid behov informera övriga verksamheter, som perifert kan påverkas.

Av krishanteringsplanen framgår också att IT-levererande part har skyldighet att utforma krishanteringsklausul och avbrottsplan i avtal mellan leverantör av tjänster/varor och Västra Götalandsregionen, samt att vid behov ingå i berörda verksamheters krisorganisation.

10.6 Uppföljning av incidenter

Uppföljning av informationssäkerhetsincidenter ska ske i två olika nivåer:

- Uppföljning av enskilda incidenter, enligt rutin för VGR:s system för avvikelsehantering. För att kartlägga bland annat orsak, förlopp och vilka eventuella ytterligare säkerhetsåtgärder som kan behövas för att förhindra att liknande incidenter inträffar. Ansvaret följer linjeansvaret.
- Analys av statistik över incidenter, för att få en samlad bild, urskilja eventuellt mönster och systematiska felkällor och möjliga förbättringsåtgärder.

10.7 Rapportering av händelser

Händelser av större och/eller allvarligare karaktär ska analyseras och rapporteras till Koncernkontorets säkerhetsenhet. På begäran av koncernsäkerhetschefen ska det genomföras en händelse-/orsaksanalys och, där detta bedöms adekvat, rapporteras till regionstyrelsen.

11 KONTINUITETSPLANERING

11.1 Mål

Det ska finnas kontinuitetsplanering, för att säkerställa tillgång till information och funktioner som krävs, för att upprätthålla av ledningen prioriterad verksamhet. Planeringen ska regelbundet testas och uppdateras.

11.2 Utgångspunkt

Med kontinuitetsplanering avses den planering som behövs för att minimera de negativa effekter, som kan bli resultatet av olika typer av avbrott i tillgång till informationen. Avbrotten kan vara av olika karaktär, allt från mindre störningar till katastroftillstånd.
Avsikten med planeringen är att upprätthålla kritiska verksamhetsprocesser och, så snabbt som möjligt efter ett avbrott, återgå till normalläge med korrekt och fullständig information.

11.3 Arbetet med kontinuitetsplanering

Inom ramen för verksamhetens arbete med kontinuitetsplanering ska en konsekvens- och riskanalys genomföras, för att identifiera kritiska verksamhetsprocesser och krav på kontinuitet för dessa. Därefter ska organisationen identifiera vilka informationstillgångar, samt nivåer av tillgänglighet, riktighet, sekretess och spårbarhet, som krävs för att de verksamhetskritiska processerna ska fungera som avsett. Även beroenden till nyckelpersoner för att upprätthålla verksamheten ska identifieras och dokumenteras i detta arbete.

Arbetet ska generera en kravspecifikation för verksamhetsprocesserna, som definierar krav på återstartstider samt maximal toleranstid för förlust av data vid ett avbrott. Att definiera krav på återstartstid innebär den maximala tid som en aktuell process tillåts vara otillgänglig.

Kravspecifikationen ska sedan utgöra underlag för vilka kontinuitetslösningar som väljs och hur reservrutiner ska utformas.

Kontinuitetsplaneringen ur informationssäkerhetssynpunkt innehåller två delar. En del är verksamhetens kontinuitetsplan. Den andra delen är den avbrottsplan som IT-levererande part och övriga resursägare ska ha och som ska svara mot verksamhetens ställda krav.

Planerna ska finnas tillgängliga i olika format, för att säkra åtkomst vid händelse. Men även förvaras skyddat, så att inte känslig information blir åtkomlig för obehöriga.

Kontinuitetsplanen ska fortlöpande stämmas av med verksamhetens krishanteringsplan, för att säkerställa att dessa fungerar effektivt tillsammans.

Kontinuitetsplanen ska regelbundet testas/övas, utvärderas och revideras.

11.4 Verksamhetens ansvar

Förvaltningschef ska, som grund för kravställning mot IS/IT-leverantören, identifiera kritiska verksamhetsområden och informationsprocesser. Syftet är att i samband med störningar och krissituationer kunna prioritera och säkerställa verksamhetens funktionalitet.

I verksamhetens kontinuitetsplan ska ingå manuella rutiner för alternativ drift utan informationssystem. Personal ska utbildas i dessa och rutiner ska årligen testas.

11.5 Informationsägarens ansvar

Informationsägaren ansvarar för att kontinuitets- och avbrottsplan harmoniserar med varandra.

11.6 Resursägarens ansvar

Resursägaren ansvarar för att upprätta en avbrottsplan, som tar sin utgångspunkt ifrån verksamhetens prioritering och informationsklassificering

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.

BILAGA 1 - TERMER OCH DEFINITIONER

För användningen av detta dokument gäller följande termer och definitioner:

Allvarlig händelse
Händelse som är så omfattande att resurserna måste organiseras, ledas och användas på särskilt sätt. (Krishanteringsplan Västra Götalandsregionen)

Avbrottsplan
Resursägarens planering för att åtgärda olika typer av avbrott i infrastruktur och teknik. Avbrottsplanen ska utgå från verksamhetens prioritering och informationsklassificering

Behörighet
En persons åtkomsträttigheter till information i IT-system

Hot
Möjlig, oönskad händelse med negativa konsekvenser för verksamheten

Information
Innebörd hos data

Informationsbehandlingsresurser
Informationsbehandlingssystem, -tjänst eller stödjande infrastruktur, eller lokaler som inhyser resurserna.

Informationssäkerhet
Säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet (även spårbarhet och oavvislighet)

Informationssäkerhetsincident
En enskild eller en serie av oönskade eller oväntade informationssäkerhetshändelser som har en signifikant sannolikhet att äventyra verksamheten och hota informationssäkerheten

Informationstillgång
En organisations information och de resurser som används för att hantera informationen.
*Exempel på informationstillgång är: Information (kunddatabas, metodik, dokument etc.), program (applikation, operativsystem etc.), tjänster (Internetförbindelse, elförsörjning etc.), fysiska tillgångar (dator, bildskärm, telefon etc.). Informationstillgång kan vara av fysisk eller logisk karaktär, eller båda*dera

Informationsägare
En aktör som ansvarar för informationen. Informationsägarskapet definieras och utses i respektive organisation.
Regionstyrelsen är ägare av regionens samlade informationstillgångar Respektive nämnd, styrelse och bolagsstyrelse företräder regionen inom sitt ansvarsområde och ansvaret följer ordinarie linjeansvar. Företräds, i tillämpliga delar, av Objektägare verksamhet när informationen ingår i ett av regionens förvaltningsobjekt för IS/IT

Inre sekretess
Området för inre sekretess innefattar samtliga vårdenheter som ingår i VGR *(25 kap 11 § punkt 2 Offentlighets- och sekretesslagen)*. Privata vårdgivare och gemensamma nämnder ligger utanför.
Vid inre sekretess görs ingen sekretessprövning enligt sekretesslagen. Det är användaren själv som gör bedömningen och har ansvaret, att legala kraven och verksamhetschefs regler följs och att endast ta del av de patientuppgifter som är nödvändiga för arbetsuppgiften.

IT-säkerhet
Säkerhet beträffande IT-system med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation

Konfidentialitet (insynsskydd)
Avsikten att innehållet i ett informationsobjekt (eller ibland även dess existens) inte bör göras tillgängligt eller avslöjas för obehöriga

Kontinuitetsplan
Dokument som beskriver hur verksamheten skall bedrivas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas eller störs under en längre, specificerad tidsperiod.
Avsikten med planen är att upprätthålla kritiska verksamhetsprocesser och, så snabbt som möjligt efter ett avbrott, återgå till normalläge med korrekt och fullständig information.

Objektägare verksamhet, /-ledare, -samordnare, -specialist
Roller inom regionens styr- och förvaltningsmodell för IS/IT, som företräder verksamhetssidan

Objektägare IT, /-ledare, -samordnare, -specialist
Roller inom regionens styr- och förvaltningsmodell för IS/IT, som företräder tekniksidan

Personuppgift
All slags information, som direkt eller indirekt kan knytas till en fysisk person som är i livet. Även bild- och ljuduppgifter om fysisk person räknas som personuppgifter, även om inga namn nämns. Krypterade eller kodade uppgifter är också personuppgifter, om någon har en nyckel som kan koppla dem till en person

Personuppgiftsansvarig
Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandling av personuppgifter

Personuppgiftsombud
Den fysiska person som, efter förordnande av personuppgiftsansvarig, självständigt ska se till att personuppgifter behandlas på ett korrekt och lagligt sätt och i enlighet med god sed samt genomföra revision

Policy
Dokument som beskriver ledningens viljeinriktning. Beskriver ”Att” och ”Varför”.

Resursägare
Är den som äger teknik, infrastruktur eller IS/IT-tjänster. Motsvarar rollen objektägare IT om resursen ingår i regionens styr- och förvaltningsmodell för IS/IT

Riktighet
Egenskapen att skydda exaktheten och fullständigheten gällande tillgångar

Risk
Kombination av sannolikheten för att en incident ska inträffa och konsekvenserna av en denna

Riskanalys
Process som identifierar hot mot verksamheten och uppskattar storleken hos relaterade risker

Riskbedömning
Övergripande process för riskanalys och riskvärdering

Riskhantering
Samordnade aktiviteter för att styra och kontrollera en organisation med avseende på risk

Riskvärdering
Process där uppskattad risk jämförs med uppsatta riskkriterier, för att avgöra riskens betydelse

Root-konto
Är en form av administrationskonto med högsta behörighet

Skadlig kod
En generisk term för skadliga datorprogram är ”skadlig kod” Virus är en typ av skadlig kod. En besläktad företeelse är ”maskar” som inte behöver någon hjälp från användare för att spridas

Spårbarhet
Möjligheten att entydigt kunna härleda utförda aktiviteter i systemet och/eller processen till en identifierad användare eller resurs

Sårbarhet
Brist i skyddet av en informationstillgång exponerad för hot.
Detta kan t ex gälla fel i ett systems säkerhetsprocedurer men även brister i rutiner eller fysiskt skydd.

Säkerhetsåtgärd
Medel för hantering av risk, innefattandes policyer, riktlinjer, rutiner, förfaranden eller organisationsstrukturer vilka kan vara av administrativ, teknisk, ledningsmässig eller juridisk karaktär

Tillgång
Allt som är av värde för organisationen

Tillgänglighet
Skyddsmål där informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid”.

VGR-riktlinje/VGR-rutin
Beskrivning som klargör vad som ska göras och hur, för att nå målen som fastslagits i regelverken. VGR-riktlinje/-rutin är regiongemensam och beslutad på tjänstemannanivå.

Yttre sekretess
Innan uppgifter lämnas till mottagare utanför Västra Götalandsregionen görs sekretessprövning enligt offentlighets- och sekretesslagen