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