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.