VÄSTRA GÖTALANDSREGIONEN

Koncernkontoret
Enhet säkerhet

Dokumenttyp	Övergripande dokument	Version
VGR-riktlinje	Riktlinjer för informationssäkerhet	1.0
Dokumentansvarig	Kontaktperson	Dnr
Valter Lindström	Monika Göransson	RS 129-2015
Beslutad av	Giltig från	Ersätter
Valter Lindström, koncernsäkerhetschef	2015-12-08	Regional anvisning för styrning av kommunikation och drift, RSK 265-2003

VGR-RIKTLINJE FÖR KOMMUNIKATION OCH DRIFT

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.

Ur riktlinjer informationssäkerhet för Västra Götalandsregionen

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.

Ur Riktlinjer för informationssäkerhet i Västra Götalandsregionen

1 Grundförutsättning

IS/IT-direktören ansvarar för tekniska skyddsåtgärder samt operativa och administrativa driftrutiner.

Information och utrustning ska skyddas på ett likvärdigt sätt, oavsett om den hanteras innanför eller utanför regionens lokaler eller IS/IT-miljö.

2 Ansvar för säkerhet

Arbetsbeskrivningen för funktioner inom drift och förvaltning av IS/IT system ska även omfatta säkerhetsansvar både vad gäller informations- och IT-säkerhet. Detta ska beskrivas i system- och driftdokumentationen.

3 Drift- och systemdokumentation

Det ska finnas system- och driftdokumentation som tydliggör vilka skyddsåtgärder som implementerats. Det ska finnas en process som säkerställer att system- och driftdokumentationen är aktuell.

Om extern leverantör anlitas ska dokumentationen vara tillgänglig för Västra Götalandsregionen, vilket ska regleras i avtal.

Känslig dokumentation ska endast vara tillgänglig för behörig personal.

4 Övervakning av driftmiljö

I övervakningsansvaret ingår scanning av kända sårbarheter, scanning av elak kod, kontroll av trådlösa accesspunkter, kontinuerlig kontroll av administratörsrättigheter, genomlysning och rapportering av konton som inte kan associeras med en ägare eller verksamhetsprocess.

IT-system som är verksamhetskritiska ska även driftövervakas kontinuerligt och loggas för att minimera avbrott och andra IT-incidenter. Loggar ska skyddas mot radering, manipulation och obehörig åtkomst. Nivå/omfattning för övervakning ska regleras i avtal med VGR IT. I de fall annan part sköter delar av övervakningen ska detta regleras med avtal. I avtalet ska åtkomstregler och rättigheter regleras.

Informationssäkerhetsavvikelser ska dokumenteras på ett strukturerat sätt och berörd objektförvaltning samt berörda verksamheter ska informeras om relevanta informationssäkerhetsavvikelser

5 Underhåll

Alla förändringar i driftmiljöer ska riskbedömas och vid behov testats ur ett säkerhetsperspektiv.

Det ska finnas en återställningsplan, som ska kunna användas i händelse av en misslyckad förändring i driftmiljö.

Vid underhåll av driftsmiljöer ska hänsyn tas till organisationens behov av åtkomst till information för att upprätthålla verksamheten.

Det ska finnas en rutin för att hantera akuta händelser i driftmiljön. Det kan finnas tillfällen, då en ändring behöver genomföras mer brådskande och att undantag från den etablerade ändringsrutinen behöver göras. Även för denna typ av ändring ska organisationen ha en rutin som beskriver hanteringen och hur avsteget dokumenteras.

6 Godkända applikationer

I organisationens driftmiljö, intern eller extern, ska endast godkända applikationer vara aktiverade och möjliga att använda.

En aktiv kontroll av avvikelser ska ske, i syfte att säkerställa att endast auktoriserade hård- och mjukvaror finns i det interna nätverket.

7 Kontroll över anslutningar

Samtliga anslutningar till Västra Götalandsregionens interna driftmiljö ska godkännas och dokumenteras enligt VGR IT:s rutiner.

8 Fjärranslutning

Annan utrustning och/eller anslutning via andra nätverk får ske genom godkänd fjärråtkomst. Detta gäller externa avtalsparter och ska kravställas vid upphandling och beställning. Fjärrsupport kräver godkännande av VGR IT och ska hanteras enligt fastställda rutiner. Detta gäller oavsett om det är regionens medarbetare eller externa leverantörer som utför underhållsåtgärder eller på annat sätt ger stöd.

9 Skydd av VGR-net

Organisationens datakommunikation ska skyddas i enlighet med verksamhetens behov och hot från omvärlden. Det ska finnas ett regelstyrt skydd mellan regionens nätverk och andra nätverk. Med andra nätverk avses t.ex Internet, Sjunet och skolnät

9.1 Segmentering av nätverk

Fysisk och logisk segmentering av organisationens nätverk ska, som en del av regionens säkerhetsarkitektur, användas för att skydda information och övriga informationsbehandlingsresurser.

För att svara mot olika verksamhets- eller funktionsbehov – t ex medicinteknik, telefoni, medborgare, skolnät – ska segmentering kunna erbjuda olika säkerhetsnivåer.

All kommunikation mellan resurser i olika logiska nät ska vara godkända och ska dokumenteras av resursägaren.

10 Skyddad kommunikation

Vid överföring av information ska denna skyddas, enligt den skyddsnivå som svarar mot informationsklassificeringen.

Vid kommunikation av patientdata eller annan känslig information (insynsskydd klass 3–4) ska denna vara krypterad. När patientuppgifter kommuniceras över nätverk ställs legala krav på säkerhet genom kryptering. Det innebär att patientuppgifter måste överföras genom en krypterad förbindelse eller genom att kryptera uppgifterna.

11 Informationsbehandlingsresurser ska skyddas mot skadlig kod

Inom VGR ska det finnas rutiner för att upptäcka och förhindra skadlig kod, samt metoder för att återställa IT-miljön efter angrepp av skadlig kod. Då extern leverantör anlitas ska krav på säkerhetsuppdatering och skydd ingå i avtalet.

12 Penetrationstester

Interna och externa penetrationstester bör genomföras, i syfte att verifiera att säkerhetsåtgärderna har förväntad effekt. Kan initieras av IS/IT-direktören eller säkerhetsdirektören.

13 Vid misstanke om brott

Loggning i driftmiljön skall ge förutsättning för att händelsekedjor kan återskapas vid misstanke om brott.

14 Säker plattform för mobila enheter

Används mobila enheter som kopplas till VGR-net, ska regionens säkerhetsarkitektur användas. Mobila enheter är t ex telefoner, bärbar pc, läsplattor, distansarbetsplatser. Det är väsentligt att informationen har likvärdigt skydd även i mobila enheter.

15 Publika datorer

Dator tillgänglig för besökare, patienter m fl ska vara logiskt skild från kärnverksamhetens nätverk.

16 Organisationen ska skyddas från förlust av information

Organisationen ska skyddas från förlust av data genom en formaliserad rutin och implementerad teknik för säkerhetskopiering.
Rutinen ska bl.a. innehålla:

- Verksamhetskrav, periodicitet
- Ansvarsfördelning mellan IT och verksamhet
- Backup rutin och teknik
- Förvaring av säkerhetskopior
- Versionshantering av säkerhetskopior
- Återläsningsrutiner

För att säkerställa att säkerhetskopiering och återläsning fungerar på avsett sätt, ska regelbundna kontroller och verifieringar göras.

Då extern part anlitas, ska beställaren avtala om att kraven på säkerhetskopiering, lagring och förvaring tillgodoses.

Säkerhetskopia av data ska förvaras så att geografiskt lokala incidenter eller katastrofer inte äventyrar åtkomsten till eller riktigheten i säkerhetskopierad data. Säkerhetskopia av data ska förvaras så att inte obehörig åtkomst kan ske och sparas enligt rutin, på ett sätt som uppfyller verksamhetens krav.

17 Avveckling av IS/IT-resurser

Funktioner och tjänster i driftmiljön som inte används ska avinstalleras eller avaktiveras. Oanvända system och funktioner är en känd sårbarhet, som kan utnyttjas för otillåtetet intrång i VGR:s IT-miljöer.

När IT-utrustning utrangeras, kasseras, säljs eller på annat sätt lämnar VGR ska det finnas instruktioner och rutiner för detta.

Alla öppningar i organisationens perimeterskydd ska återställas när en IS/IT-resurs avvecklas.

Vid avveckling av IS/IT-resurs ska informationen omhändertas enligt Regionarkivets regler och rekommendationer. Lagringsmedia ska alltid förstöras, avmagnetiseras eller överskrivas på ett säkert sätt. Licensierade program ska raderas.

Då externa leverantörer anlitas, ska villkoren för avveckling ingå i avtalet.