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 systemutveckling och systemunderhåll, RSK 265-2003

VGR-RIKTLINJE FÖR STYRNING AV UTVECKLING OCH INFÖRANDE AV IS/IT

Mål

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

Ur Informationssäkerhetspolicy för Västra Götaland

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.

Ur Riktlinjer för informationssäkerhet i Västra Götalandsregionen

1 Allmänt

Detta kapitel beskriver aktiviteter för utveckling och underhåll av IT-system och syftar till att säkerställa verksamhetens krav på informationssäkerhet.

2 Anskaffning, utveckling och underhåll av IT-system ska ske på ett kontrollerat sätt

Det ska finnas en tydlig process från att ett behov identifierats till att en lösning godkänts och kan börja användas i ordinarie drift. I kravspecifikationen för nya system eller utökning av befintliga system ska kraven säkerheten specificeras. Säkerhetskrav och åtgärder ska spegla värdet av de berörda informationstillgångarna. Vid utvecklingsprojekt för system- och tillämpningsapplikationer är det den projektansvarige som ansvarar för att riskanalyser genomförs. Vid större projekt ska även risker för själva projektet analyseras och hanteras.

Om den planerade lösningen påverkar andra informationsägares eller verksamheters informationssäkerhet ska projekt-/systemägaren bedöma, behandla och informera om identifierade risker. För varje IT-leverans ska det verifieras att design av den nya lösningen tar hänsyn till identifierade beroenden till andra system eller infrastruktur inom och utanför organisationen

Det ska finnas en teststrategi för leverans av IT-system, som även ska omfatta säkerhetstester.

Det ska i kravspecifikationen definieras vilken dokumentation som ska levereras. Dokumentationen ska minst omfatta system- och driftdokumentation

3 Systemägaren ska bedöma behovet av tillgång till och skydd av källkod.

För upphandlade system eller system utvecklade av extern leverantör ska källkoden om möjligt och vid behov deponeras hos extern förtroendeman och avtal slutas om att systemägare har rätt att nyttja källkoden om upphovsrättsinnehavaren avslutar sitt åtagande.

4 Systemutveckling ska ske under kontrollerade former

VGR:s projektmodell och metoder ska säkerställa att verksamhetens säkerhetskrav uppfylls. Särskild vikt bör läggas vid kravställning på externa leverantörer och nationella e-Hälsotjänster. Om extern leverantör anlitas för utvecklingsinsatser ska det i avtal definieras vilken dokumentation som ska överlämnas till beställaren vid projektets avslutande.

I utvecklingsarbetet ska behovet av kompetens inom informationssäkerhet tillgodoses.

5 Upphandling av produkter och tjänster ska alltid genomföras enligt fastställd rutin för upphandling.

Inköpsprocessen/rutinen ska säkerställa att leverantörer värderas utifrån sin förmåga att leva upp till organisationens informationssäkerhetskrav. Det är viktigt att definiera vad som upphandlas eftersom ansvarsförhållandena ser olika ut vid exempelvis upphandling av en applikation jämfört med upphandling av en molntjänst. Exempelvis personuppgiftsbiträdesavtal (PUB-avtal), säkerhetsskyddsavtal.

Leverantörens skyldighet att leva upp till VGR:s informationssäkerhetskrav ska dokumenteras i avtal. Om den leverantör som VGR väljer att ingå avtal med på någon punkt inte förmår leva upp till säkerhetskraven ska den risk som uppstår ur avvikelsen analyseras och åtgärder för att minska risken godkännas, av ansvarig ägare till informationsbehandlingsresursen, innan avtalet sluts.

Verksamhetens behov av skyddsåtgärder ska vara en del av förfrågningsunderlaget vid en upphandling av en ny tjänst, produkt eller vid vidareutveckling eller avveckling. Vid varje leverans ska det kontrolleras att beslutade skyddsåtgärder är genomförda och godkända.

Det kan finnas tillfällen då det av olika skäl måste göras avsteg från beslutade skyddsåtgärder i arbetet med att ta fram en lösning som VGR har beställt. I alla sådana situationer skall avsteget analyseras med avseende på vilken risk avsteget innebär och vilka åtgärder som behöver vidtas för att hantera risken.

6 Utvecklings- och testarbete

Allt utvecklings- och testarbete ska ske på ett sådant sätt att inga nätverkskomponenter, applikationer eller användare kan påverka produktionsmiljöerna.

6.1 Säkerhet i utvecklings- och underhållsprocesser

För att uppnå och bibehålla säkerhet i tillämpningssystem och information ska projekt- och underhållsmiljöer styras noga. De ska säkerställas att alla föreslagna systemändringar granskas för att kunna kontrollera att de inte äventyrar säkerheten vare sig i systemet eller i driftmiljön.

6.2 Utvecklings, test och utbildningsmiljö

Miljöer för utveckling, test och utbildning ska vara skilda från produktionsmiljön. Under mycket speciella omständigheter, då de olika miljöerna inte kan hållas åtskilda, kan IS/IT-direktör medge undantag.

Skarp data får inte användas i utbildningssammanhang och testdata ska vara avidentifierade eller skapade för avsedda ändamålet. Utvecklings- och testdata ska avidentifieras så att det inte går att utläsa uppgifter som kan härledas till en person.

6.3 Teknisk granskning av förändringar i produktionssystem

Ibland är det nödvändigt att ändra produktionssystemet, t.ex. installera nya programversioner eller programändringar. När sådana ingrepp görs bör säkerhetssystemen kontrolleras och testas för att säkerställa att inte drift och säkerhet påverkas negativt.

6.4 Säkerhetstest

Ändringar i informationsbehandlingsresurser ska riskanalyseras och vid behov säkerhetstestas innan produktionssättning.
Resultatet av genomförda säkerhetstester ska vara godkända, av IT-säkerhetsansvarig och den som är ansvarig för den resurs som testerna avser, innan en driftsättningsanalys genomförs.
Tester ska utgå från fastställda krav på informationssäkerhet. Projektägaren ansvarar för att säkerhetsåtgärder genomförs inför säkerhetstest och driftsättningsanalys samt att relevant dokumentation medföljer.

6.5 Driftsättningsanalys externa IT-tjänster

VGR ska kravställa utförare av nationella IT-tjänster att beslutad rutin/process för driftsättning ska var genomförd och vara godkänd av informationsägare innan produktionssättning genomförs.

6.6 Driftsättningsanalys interna IT-tjänster

Driftsansvarig inom VGR IT ansvarar för att det, tillsammans med informations- och resursägaren, genomförs en driftsättningsanalys. Driftsättningsgodkännandet ska vara dokumenterat och godkänt av båda parter.