Rutin

Gäller för: Västra Götalandsregionen
Innehållsansvar: Jakob Sandberg, (jaksa4), Regionutvecklare
Godkänd av: Johan Flarup, (johfl), Direktör

Giltig från: 2025-07-14
Giltig till: 2029-10-04

Säker drift av IS/IT

Regional rutin 2025-2029

Ledningssystem för informationssäkerhet och dataskydd

Rubrik: Säker drift av IS-IT regional rutin 2025-2029
Dokument-ID: RS10162-1596316381-367
Version: 1.0

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

1 Inledning

IT-säkerhet i driftmiljö innebär att säkerställa att IS/IT-tjänsten och dess datahantering är skyddade mot oavsiktliga eller avsiktliga hot och intrång. IT-säkerhet omfattar implementering av säkerhetsåtgärder för att förebygga, upptäcka och hantera hot såsom dataintrång, skadlig programvara, obehörig åtkomst och systemavbrott, samt att etablera en snabb återhämtningsförmåga för IS/IT-tjänster. Säkerhetsåtgärder inkluderar exempelvis nätverkssäkerhet, datakryptering, åtkomstkontroll, incidenthantering samt regelbunden uppföljning av säkerhetsåtgärder.

Information och informationsbehandlingsresurser ska skyddas på ett likvärdigt sätt, oavsett om det hanteras innanför eller utanför regionens lokaler eller IT-miljö, detta inkluderar molntjänster.

Regional rutin för säker drift samlar styrning av ett stort antal säkerhetsåtgärder från ISO 27002 runt drift av IS/IT.

Rutinen är styrande för alla förvaltningar och bolag i Västra Götalandsregionen (VGR) och ingår som en del i ledningssystemet för informationssäkerhet och dataskydd (LISD).

Koncernstab digitalisering ansvarar för att ta fram kompletterande regionala tillämpningsanvisningar för verksamhet som ansvarar för drift av IS/IT (i denna rutin kallat driftsverksamhet).

2 Ansvar och roller

Ansvar och roller inom informationssäkerhet och dataskydd styrs av *Informationssäkerhet och dataskydd- Regional riktlinje 2023-2027.*

2.1 Digitaliseringsdirektör

Digitaliseringsdirektören ansvarar för att upprätta och tillhandahålla en tjänsteportfölj med säkerhetsåtgärder som matchar informationsklassning. Säkerhetsåtgärder ska användas för både internt och externt driftade IS/IT-tjänster. Digitaliseringsdirektören ansvarar också för att koncernstab digitalisering upprättar tillämpningsanvisningar för att uppfylla säkerhetsåtgärderna i LISD.

2.2 Informationsägare

Informationsägaren eller dess företrädare ansvarar för att genomföra de grundläggande informationssäkerhets- och dataskyddsanalyserna:

- Informationsklassning
- Riskhantering
- Tröskelanalys
- Konsekvensbedömning

Dessa ligger till grund för vilka krav som informationsägaren behöver ställa på IS/IT-tjänsten.

2.3 Ägare IS/IT-tjänst

Ägare av IS/IT-tjänst har som ansvar att, utifrån de krav som ställs på tjänsten genom informationsklassningen och utifrån de risker som identifierats införa, förvalta, följa upp och utvärdera säkerhetsåtgärder i IS/IT-tjänsten så att adekvat skydd uppnås.

Vid överlämning till drift flyttas ansvar över från projektägare till ägare IS/IT-tjänst. Samtliga införda och planerade säkerhetsåtgärder övertas av ägare IS/IT-tjänst. En utpekad ägare för IS/IT-tjänst ska finnas på plats före driftsättning.

Där inte specifikt ansvar pekats ut i rutinen är det ägare IS/IT-tjänst som ansvarar för att säkerhetsåtgärder är implementerade för IS/IT-tjänsten.

3 Termer och begrepp

Huvuddelen av termer och begrepp är hämtade från MSB termbank för informationssäkerhet, ISO Online Browsing Platform och andra rutiner under *Informationssäkerhet och dataskydd – Regional riktlinje 2023-2027*.

Acceptanstestmiljö	Miljö för test och verifiering av olika acceptanskriterier innan driftsättning. Kallas även acceptans, stage, pre-prod och QA även om dessa kan ha viss skillnad i betydelser.
Avvikelse	Icke-uppfyllande av ett informationssäkerhets- eller dataskyddskrav.
Drift	Övervakning, underhåll och administration av hårdvara, programvara och nätverk för att säkerställa kravställd prestanda och tillgänglighet. Kallas även IS/IT-drift.
Driftverksamhet	All verksamhet inom VGR som ansvarar för drift av IS/IT.
Informations-behandlingsresurs	Informationsbehandlingsresurs syftar på en digital eller fysisk resurs för behandling av information. En informationsbehandlingsresurs är

	vanligtvis digital, t.ex. IT-system, tjänst, infrastruktur, men kan även vara en fysisk resurs, t.ex. ett säkerhetsskåp eller en människa. På VGR motsvarar detta exempelvis digitala resurser, en IS/IT-tjänst, en stödjande tjänst eller en produkt.
IS/IT-tjänst	Är en avgränsning av en eller flera digitala informationsbehandlingsresurser. Exempelvis IT-system, applikation, mjukvara, nätverk, lagringssystem eller infrastruktur.
IT-säkerhet	En del av informationssäkerhet avgränsad till IT-resurser som servrar, hårdvara och mjukvara. IT-säkerhet berör konfidentialitet, riktighet och tillgänglighet.
IT-miljö	En samling informationsbehandlingsresurser som används för att skapa, bearbeta, lagra och distribuera information inom en organisation.
Redundans	Tillstånd då mer än ett medel finns för att upprätthålla ett givet funktionssätt syftande till att säkerställa kontinuerlig drift. Oftast åstadkoms redundans genom dubblering av kritiska funktioner. Exempel kan vara

	dubblerad elförsörjning, lagringsenheter med mera.
IT-säkerhets-specifikation	Ett dokument som tydliggör vilken nivå av säkerhet en IS/IT-tjänst har och beskriver de säkerhetsåtgärder som är implementerade.
Säkerhetskopia	Kopia av information som skapats för att kunna nyttjas vid förlust av hela eller delar av den ursprungliga informationsmängden. På svenska används ofta den engelska termen "backup"
Säkerhetsåtgärd	Säkerhetsåtgärd för informationssäkerhet omfattar organisatoriska, personrelaterade, tekniska och fysiska åtgärder för att bibehålla och/eller förändra risker. Exempel: Genomförande av kryptering för att skydda känslig information, införande av brandväggar för att säkra nätverksåtkomst eller implementering av regelbundna utbildningar för medarbetare om säkerhetsmedvetenhet.
Tillämpnings-anvisning	Dokumentation som beskriver hur säkerhetsåtgärder tillämpas i praktiken.

Åtkomstkontroll	Funktioner i ett system som syftar till att reglera och kontrollera en användares åtkomst till information och resurser
Övervakning	Bestämning av status hos ett system, en process eller en aktivitet. För att bestämma status kan det vara nödvändigt att kontrollera, ha uppsikt över eller kritiskt observera.

4 Livscykelhantering av säkerhetsåtgärder

Vid livscykelhantering av säkerhetsåtgärder för IS/IT-tjänst ska följande aktiviteter genomföras:

- Informationsägare ska tillsammans med ägare IS/IT-tjänst identifiera eventuella risker och hantera dessa enligt VGR:s process för riskhantering.
- Informationsägare ska säkerställa att informationsklassning utförs enligt rutin för informationsklassning.
- Informationsägare ansvarar för att informationshanteringsplanen (IHP) följs.
- Ägare IS/IT-tjänst ska säkerställa att säkerhetsåtgärder som berör tjänsten regelbundet utvärderas.
- Ägare IS/IT-tjänst ska säkerställa att förändringar av IS/IT-tjänsten följer en etablerad process för ändringshantering.

4.1 Kravställning

För en enhetlig och komplett kravställning gällande informationssäkerhet behövs återanvändbara krav som ska

användas vid nyutveckling, upphandlingar och förändring för att uppfylla säkerhetsåtgärder. Enskilda krav ska ha en ägare för att säkerställa att de är uppdaterade och fortsatt relevanta.

Krav gällande informationssäkerhet ska samlas i ett regionalt kravbibliotek som ska tillhandahållas av Koncernstab digitalisering.

4.2 Säker utveckling

För informationssäkerhet vid verksamhetsutveckling i VGR finns *Säker utveckling - informationssäkerhet & dataskydd vid verksamhetsutveckling- Regional rutin 2024-2028*. När ett utvecklingsuppdrag är färdigställt och överlämnas till mottagare inom drift blir denna rutin aktiv och ansvaret för säkerhetsåtgärder övergår från projektägare till ägare IS/IT-tjänst.

4.3 Ändringshantering

Ägare IS/IT-tjänst, på uppdrag av informationsägare, ansvarar för att genomföra ändringar.

Införandet av nya system och större ändringar i befintliga system ska följa överenskomna regler och en formell process för dokumentation, kravspecificering, testning, kvalitetskontroll och styrt införande i verksamheten.

Ändringshantering ska tillämpas för att säkerställa konfidentialitet, riktighet och tillgänglighet för information i informationsbehandlingsresurser och informationssystem under hela livscykeln för systemutveckling, från tidiga designfaser och hela vägen genom alla därpå följande underhållsinsatser.

4.4 Driftsättning av IS/IT-tjänst

Före driftsättning av IS/IT-tjänst påbörjas finns det krav som måste säkerställas av projektägare för att begränsa de risker som kan uppstå vid driftsättning.

- Riskerna kring den nya IS/IT-tjänsten måste dokumenteras och hanteras enligt regional mall riskhantering för informationssäkerhet.
- Före driftsättning sker ska det finnas en strategi för att återställa miljön installationen skedde i.
- Gällande test- och releaseprocess ska följas.
- Före driftsättning sker ska nya system/applikationer vara testade och godkända för produktionssättning enligt en ändringshanteringsplan.
- Ägare av den nya IS/IT-tjänsten ska finnas i samband med driftöverlämning.
- Det nya systemet ska läggas till i relevant förteckning av informationstillgång.
- Informationsägare och eventuella andra identifierade riskägare ska informeras av projektägare om driftöverlämningen och systemets säkerhetsspecifikation för fortsätt hantering av risker.

4.5 Installation av programvara i driftsatta system

Säker installation av programvara i driftsatta system minskar misstag i driftmiljöer och risken för att tekniska sårbarheter utnyttjas. Uppdateringar ska alltid prioriteras om de avlägsnar allvarliga eller kritiska sårbarheter[1].

[1] Sårbarheter värderas efter CVSS skala.

Ägare av IS/IT-tjänst ansvarar för att åtgärder säkerställer integriteten hos driftsatta system och förhindrar att tekniska sårbarheter utnyttjas. Åtgärder ska säkerställa följsamhet till relevanta delar av *ISO/IEC 27002, avsnitt 8.19*.

- Installation eller uppdatering får enbart ske efter slutförd ändringshantering.
- Enbart granskad, kompilerad och exekverbar kod ska installeras i driftsatta system.
- I samband med installation ska berörda programbibliotek uppdateras.
- Gällande test- och releaseprocess ska följas.
- Före förändringar sker ska en strategi för att återställa systemet skapas.
- All nyinstallation ska dokumenteras med versionshistorik.

4.6 Kontinuerlig leverans

Automation ska användas där så är möjligt. Det är viktigt för att kunna köra tester och verifieringar ofta, konsekvent och heltäckande. Kontinuerlig integration och kontinuerliga leveranser är viktiga verktyg för att åstadkomma detta och minska personberoende och den mänskliga faktorn.

4.7 Kapacitetshantering

Resursanvändningen i driftmiljö ska övervakas och justeras enligt gällande kapacitetskrav i syfte att kunna säkerställa kapacitet hos informationsbehandlingsresurser.

Resursanvändning i driftmiljö syftar till att den kapacitet och prestanda som krävs av informationsbehandlingsresurser tillgängliggörs samt att, där det är möjligt, radera data som inte längre behövs. Data som tas bort på grund av kapacitetsproblem får inte strida mot gällande regler för informationshanteringsplan (IHP).

Verksamhet som ansvarar för drift ska tillgodose tillräcklig kapacitet i driftmiljöer. Ägare av en IS/IT-tjänst ansvarar för kapacitetsplanering för sin tjänst i samråd med driftverksamhet och informationsägare för att tillgodose kapacitetsbehov under tjänstens livscykel.

Åtgärder ska säkerställa följsamhet till relevanta delar av *ISO/IEC 27002, avsnitt 8.6*.

För att uppnå en adekvat kapacitetshantering ska följande utföras:

- Analysera belastning och belastningsmönster för system och tjänster samt identifiera nuläge och börläge för kapacitetsbehov, prestanda och tillgänglighet (belastningsanalys).
- Övervaka och utvärdera kapacitetsbehov för lagring, prestanda och annan resursanvändning.
- Agera på monitorering och utvärderingar för att proaktivt implementera åtgärder kopplat till överbelastning och prestandaproblem. Säkerställ att tillräcklig skalbarhet finns för system och tjänster utefter kapacitetsbehov.
- Utföra belastning- och tillgänglighetstester vid större förändringar.
- Dokumentera och uppdatera belastningsanalys, avvikelser och åtgärder när det är lämpligt eller när system, teknik eller arbetsmetoder förändras.
- Tillämpningsanvisning ska finnas som beskriver hantering och optimering av lagringsmedia och avveckling av ej använda resurser.

4.8 Avveckling av system

Process för avveckling IS/IT[2] ska följas inför och under avveckling av system. Information ska omhändertas eller gallras enligt informationshanteringsplan (IHP) i Västra Götalandsregionen.

Lagringsmedier som innehåller konfidentiell eller upphovsrättsskyddad information och som ska flyttas, återanvändas, avvecklas och/eller återvinnas ska informationen först förstöras, tas bort eller skrivas över för att göra den ursprungliga informationen omöjlig att återskapa. Det ska även bekräftas att samtlig information relaterat till personuppgifter som kan finnas lagrad i minne eller andra lagringsenheter har raderats permanent. För säker avveckling ska lagringsmedier som kan innehålla personuppgifter behandlas som om den faktiskt innehåller personuppgifter.

Åtgärder ska säkerställa följsamhet till relevanta delar av *ISO/IEC 27002, avsnitt 7.14*.

5 Miljöer

För att skydda produktionsmiljö och produktionsdata från negativ påverkan till följd av utvecklings- och testverksamhet ska miljöer för utveckling, testning och produktion i normalfallet skiljas åt. Separation minskar risk för och konsekvenser av misstag.

För att skydda IT-miljöer ställs även krav på fysisk säkerhet som skalskydd, brandskydd och klimatkontroll i de lokaler där servrar och annan viktig hårdvara är placerad. För att möjliggöra en säker drift är det grundläggande att driftlokalerna är adekvat skyddade mot fysiska hot.

[2] Information finns på intranätet under “Avveckling IS/IT”. https://insidan.vgregion.se/stod-och-tjanster/amnen-a-o/digitalisering/avvecklingisit/

Koncernstab digitalisering ansvarar för att ta fram tillämpningsanvisning som säkerställer följsamhet till avsnitt 8.31 i ISO/IEC 27002.

5.1 Separation av utvecklings-, test- och produktionsmiljöer

VGR ska vid drift säkerställa en tydlig åtskillnad mellan olika IT-miljöer för att undvika oavsiktlig påverkan av produktionsmiljön från utvecklings- och/eller testaktiviteter.

5.1.1 Utvecklingsmiljö

Utvecklare behöver kraftfulla verktyg och utökade behörigheter för att göra sitt jobb vilket gör utvecklingsmiljö mer utsatt.

Minst följande säkerhetsåtgärder ska följas i utvecklingsmiljö:

- Utvecklare ska använda verktyg för kodanalys och sårbarhetsskanning.
- Utvecklingsmiljöer ska vara separerade från produktionsmiljöer för att minska oavsiktliga påverkan.
- Kompilatorer, editorer och andra utvecklingsverktyg eller verktygsprogram ska inte vara tillgängliga från produktionsmiljö när det inte är nödvändigt.

5.1.2 Testmiljö

Testmiljöer ska användas för att testa och verifiera allt från enskilda komponenter till hela system och integrationer mellan system. Testmiljöer kan ha olika namn beroende på vad syftet med dem är. Vanliga namn är acceptans, stage, pre-prod och QA.

Testmiljöer är en väsentlig del av en fungerande och säker releasekedja. En testmiljö för IS/IT-tjänst ska efterlikna motsvarande produktionsmiljö för tillförlitliga tester och upptäckt av sårbarheter innan överföring till produktionsmiljö.

Produktionsdata ska inte existera i testmiljöer utan att först pseudonymiseras eller anonymiseras.

5.1.3 Produktionsmiljö

Produktionsmiljö ska enbart användas för IS/IT-tjänster i produktion. Det betyder att applikation under utveckling, uppdateringar, förändring av konfigurationer osv. först testas och valideras i testmiljöer innan den tar sig till produktion. Installation och uppdatering ska ske efter tillräckligt omfattande och lyckade tester.

6 Kontinuitet

Kontinuitet innebär förmågan att upprätthålla och säkerställa ständig verksamhet och tillgänglighet i organisationen. En effektiv kontinuitetsplan inkluderar identifiering av risker, utveckling av åtgärder samt att minimera oplanerade avbrott i system och applikationer. Kontinuitetsarbetet i VGR styrs av *Kontinuitet - Regional riktlinje 2023 – 2027* samt *Kontinuitetshantering av IS/IT-tjänst- Regional rutin 2023-2027*

6.1 Säkerhetskopiering av information

All information som är viktig för VGR:s verksamheter behöver säkerhetskopieras, också känt som backup, för att kunna säkerställa återställningsförmåga. Åtgärder ska säkerställa följsamhet till relevanta delar av ISO/IEC 27002, avsnitt 8.13.

Det ska finnas en grundnivå för verksamhetsinformation som inte särskilt klassats och kravställts. Denna grundnivå motsvarar säkerhetskopiering minst dygnsvis med en månads bevarade säkerhetskopior.

Nivån på och frekvens av säkerhetskopiering, bevarande och återställning av information avgörs av informationsklassningens

nivå för tillgänglighet samt skyldigheter som följer av NIS 2 och andra lagkrav. Information som är kritisk och som behöver utökad säkerhetskopiering måste vara klassad enligt *Informationsklassning- Regional rutin 2024-2028* och dokumenterat i avtal med driftverksamhet (ex SLA, OLA). Olika typer av säkerhetskopiering, inklusive fullständig, differentiell och inkrementell, ska implementeras beroende på krav och resursbegränsningar.

Åtgärder att överväga inkluderar, men är inte begränsade till:

- Skydda säkerhetskopior med likvärdigt skydd som originalinformationen
- Fysiskt skydd för lagring av säkerhetskopierade data
- Separation av säkerhetskopior och produktionsdata
- Återställningsplaner
- Övervakning av säkerhetskopiering
- Felhantering vid säkerhetskopiering
- Säkerhetskopiering och återställning ska kontinuerligt testas, utvärderas och förbättras

Ytterligare krav tillkommer när säkerhetskopiering involverar personuppgifter. Dessa åtgärder gäller även när personuppgifter behandlas av extern part:

- Tillhandahålls en tjänst som hanterar personuppgifter i säkerhetskopia ska kunden informeras om vilka personuppgifter som kopieras och potentiella begränsningar av säkerhetskopior
- När personuppgifter återställs måste riktigheten i personuppgifterna garanteras och potentiella fel måste identifieras och åtgärdas. Att åtgärda potentiella fel kan behöva involvera den registrerade individen
- Återställningsarbete ska loggas. Loggen måste minst innehålla namn på den person som är ansvarig för återställning och en beskrivning av de personuppgifter som återställs

6.2 Redundans för informationsbehandlingsresurser

Informationsbehandlingsresurser ska ha tillräcklig redundans för att uppfylla gällande krav på tillgänglighet. Redundans, eller dubblering, gäller inte enbart data utan kan omfatta alla mjukvarubaserade eller fysiska komponenter som utgör informationsbehandlingsresurser såsom hela eller delkomponenter av servrar, nätverk eller klientutrusning. Redundans kan vara tillgänglig och aktiv kontinuerligt eller aktiveras vid behov.

Tillämpningsanvisningar ska säkerställa följsamhet med ISO/IEC 27002, avsnitt 8.14.

7 Åtkomstkontroll

Säkerhetsåtgärder för åtkomstkontroll styrs av *Åtkomst till information och relaterade tillgångar- Regional rutin 2025-2029*.

7.1 Förhindrande av dataläckage

Dataläckage ska förhindras så att känslig information inte sprids eller röjs till obehörig. Åtgärder för förhindrande av dataläckage ska säkerställa tillämpning av ISO/IEC 27002, avsnitt 8.12.

Det är primärt informationsklassningens nivå av konfidentialitet som utgör krav på förhindrande av dataläckage. Åtgärder kan omfatta, men behöver inte vara begränsade till:

- Övervakning av kanaler för dataläckage, exempelvis e-post, mobilapplikationer, filöverföringar, bärbara lagringsenheter
- Tekniska åtgärder för hindrande av dataläckage, till exempel kopieringsskydd
- Upptäckt av pågående eller tidigare dataläckage

- Separation och regeluppsättning av informationshantering mellan domäner inom och utom organisationens kontroll

7.2 Användning av privilegierade verktygsprogram

Användning av verktygsprogram som kan ha förmåga att kringgå säkerhetsåtgärder i system och applikationer ska begränsas och styras strikt genom tillämpning av ISO/IEC 27002, avsnitt 8.18. Verksamhet som använder priviligierade verktygsprogram ansvarar för hantering av dessa. Linjechef ska godkänna behörighetstilldelning. Åtgärder kan omfatta, men behöver inte vara begränsade till:

- Begränsa användningen till minsta ändamålsenliga antal betrodda och behöriga
- Använd flerfaktorautentisering för identifiering och autentisering
- Använd fastställda och dokumenterade åtkomstnivåer för verktygsprogram
- Håll användning av verktygsprogram separerade från användning av dagliga applikationer/verktyg
- Ta bort eller avaktivera onödiga verktygsprogram
- Logga all användning av verktygsprogram

7.3 Fjärranslutning

Fjärranslutning till IS/IT-tjänster på VGR:s IT-miljö ska ske med verktyg och lösningar som är godkända av koncernstab digitalisering. Detta gäller för samtliga fjärranslutningar samt externa avtalspartner och detta ska kravställas vid upphandling. När extern avtalspartner ansluter till VGR ska deras anslutning begränsas till avtalad del av funktion och miljö.

Fjärranslutning från extern avtalspartner ska endast ha åtkomst till avtalad del.

8 Konfigurationshantering

Konfigurering och säkerhetskonfigurering av IS/IT-tjänst och tjänster inklusive hårdvara, programvara samt nätverk, ska vara implementerade, dokumenterade, övervakade och granskas regelbundet. Syftet med konfigurationshantering är att säkerställa att det som konfigureras fungerar korrekt utifrån verksamhetens behov och av skyddsnivå.

För att undvika felaktig konfiguration av IS/IT-tjänst är det viktigt att följa bästa praxis och använda strategier som minimerar risken för fel. Åtgärder ska säkerställa följsamhet till relevanta delar av ISO/IEC 27002, avsnitt 8.9. Följande åtgärder ska beaktas men inte begränsas till:

- Konfigurationsändringar ska genomföras enligt process för ändringshantering.
- Standardkonfigurationer ska finnas som säkerställer en acceptabel lägstanivå av konfiguration som hanterar organisationens behov och förutsättningar utifrån konfidentialitet, riktighet och tillgänglighet. Dessa konfigurationer ska följa branschstandard och där det är lämpligt stämmas av med leverantör.
- Förinställda konfigurationer från leverantörer, till exempel autentiseringsuppgifter, ska bytas ut innan tjänsten tas i drift.
- Konfigurationsfiler ska vara versionshanterade och förändringar ska loggas vilket underlättar att spåra ändringar och se vem som ändrade vad, när och varför.
- Där det är lämpligt och möjligt ska automatisering och orkestrering av konfigurationshanteringen tillämpas. Detta skapar enkla och fördefinierade arbetsflöden som kan utföras med begränsade behörigheter som minskar risken för mänskliga fel och förbättrar effektiviteten.

- Åtkomst till konfigurationer och information som rör konfigurationshantering ska begränsas till behörig personal.
- Konfigurationer, loggar och information som kan härledas till konfigurationsförändringar ska förvaras säkert.
- Konfigurationer och information som avser konfigurationsändringar, ska säkerhetskopieras och regelbundet testas genom återläsning.
- Konfigurationers inställningar ska utvärderas kontinuerligt. Detta underlättar upptäckt av felaktigheter och ger möjlighet att fånga upp nya användarkrav.

Åtgärder för konfigurationshantering ska säkerställa tillämpning av ISO/IEC 27002, avsnitt 8.9.

8.1 Systemhärdning

Som del av säkerhetsarbetet ska informationsbehandlingsresurser säkras genom systemhärdning. Härdning innebär att minska ett systems totala riskprofil genom att identifiera och åtgärda säkerhetsbrister. Systemhärdning ska appliceras på alla ingående komponenter i IT-miljön.

En systemhärdningsprocess innebär att man vidtar åtgärder för att säkerställa att alla aspekter av informationsbehandlingsresursen är säkrad utifrån skyddsbehov. Nedan beskrivs exempel på informationsbehandlingsresurser och exempel på systemhärdningsåtgärder som ska beaktas, men inte begränsas till:

Nätverk

- Endast behöriga enheter, samt användare, ska tillåtas att ansluta till VGR produktionsnätverksmiljö.
- Åtkomst till nätverkskomponenter ska vara baserad på principen om minsta behörighet och vara strikt reglerat.
- Kritiska och känsliga system ska isoleras.

Fler säkerhetsåtgärder som rör VGR nätverksmiljö finns att läsa i *Nätverkssäkerhet- Regional rutin 2025-2029*.

Server

- Fysiska servrar ska vara placerade i fysiskt säkra utrymmen, som låsta teknikrum eller datacenter dit endast auktoriserad personal har fysisk åtkomst. Virtuella servrar ska vara installerade på dessa fysiska servrar.
- Tjänster som inte används eller behövs för serverns avsedda funktion ska avinstalleras eller inaktiveras.
- Systemkonton ska endast ha de behörigheter som är nödvändiga för att utföra avsedd funktion.
- Firmware och drivrutiner ska vara uppdaterade med senaste rekommenderade och av VGR testade versioner.
- Datatrafik till och från serverar ska vara krypterad.

Applikation

- Behörighetsstyrning ska konfigureras för åtkomst till applikationer.
- Flerfaktorautentisering ska användas där det är tillbörligt utifrån informationstillgångens klassning.
- Åtkomstregler för autentisering och lösenord ska vara infört.
- Applikationer ska följa dess rekommenderade livscykel- och patchhantering.

Operativsystem

- Operativsystem ska hanteras enligt VGR:s livscykelplan och ska vara installerade med senaste rekommenderade och av VGR testade säkerhetspatchar.
- Verktyg för automatisk OS-uppdateringar och patchhantering ska användas. Det medför effektivare och

säkrare hantering och kan snabbt åtgärda sårbarheter samt utföra skyndsam återställning av system.
- Hårddiskar och kommunikation mellan systemkomponenter ska vara krypterad.
- Onödiga filer, bibliotek, drivrutiner och funktioner ska tas bort.
- Loggning ska vara påslagen där det är lämpligt för att upptäcka ovanlig aktivitet, fel och varningar.
- Begränsning av privilegier ska konfigureras för processer och användare.

8.2 Synkronisering av tid

Network Time Protocol (NTP) är ett protokoll som används av IS/IT-tjänster för att synkronisera systemets tid.
Tidssynkronisering gör att loggar, incidenthantering och generell drift fungerar korrekt och går att jämföra mellan olika enheter. Utan tidssynkronisering kan det bli omöjligt att följa upp en incident eller till och med att systemet inte ens fungerar i de fall där korrekt tid är extra kritiskt. Åtgärder ska säkerställa följsamhet till relevanta delar av ISO/IEC 27002, avsnitt 8.17.

- NTP eller liknande tidssynkroniseringsprotokoll ska implementeras för alla IS/IT-tjänster inom VGRnet för att säkerställa korrekt synkroniserad tid mot samma tidskälla.
- Ägare av IS/IT-tjänst och därmed konsumenter av NTP är de som har till ansvar att tidssynkronisering aktiveras på aktuell tjänst.
- Eftersom tidssynkronisering är kritisk funktion ska konfigurering ske mot både primära och sekundära NTP-servrar som enheter kan synkronisera med.
- Tidssynkroniseringen ska ske säkert och krypterat för att förhindra manipulation av tidsdata.

NTP-servrarna ska vara korrekt konfigurerade och synkroniserade med tillförlitliga tidkällor.

Problem eller incidenter relaterat till tidssynkronisering ska hanteras efter gällande incidenthanteringsprocess.

8.3 Användarklienter

Användning av användarklienter styrs i avtal och policys mellan arbetsgivare och arbetstagare. Detta kapitel uttrycker säkerhetsåtgärder enligt ISO/IEC 27002 avsnitt 8.1 som relaterar till säker drift av användarklienter.

Användarklient, så som stationär dator, bärbar dator, virtuell dator, surfplatta, mobil eller annat, vilken används i arbetet på plats eller från distans ska hållas uppdaterad med aktuella operativsystem, verktyg, virusskydd och konfigurationer. Användare ska inte vara lokal administratör på sina fysiska klienter. För virtuella miljöer (VDI) kan användare tilldelas administratörrättigheter i egen testmiljö och/eller nätverk utanför produktionsmiljö. Klienterna ska skannas efter sårbarheter och åtgärdas enligt regional rutin för hantering av sårbarheter i IT-miljö.

Vid arbete från distans ska försiktighet tillämpas gällande vilka nätverk som användarklienter kopplar upp sig mot och anvisad VPN-tunnel ska användas mot arbetsplatsen. Genom VPN och dess krypterade förbindelse kan organisationen säkerställa att användningen av mobila enheter inte automatiskt äventyrar skyddet av personuppgifter och konfidentiell information.

På användarklienter där arbetsmiljö och privat miljö samsas, ska verktygstöd kunna användas för att hindra kopiering av arbetsdata till privat miljö. Lokal lagring av känslig information ska undvikas och i den mån lokal lagring ej kan undvikas ska den ske på krypterat lagringsmedium.

Konfigurationen av användarklienter ska säkerställa följsamhet till relevanta delar av ISO/IEC 27002, avsnitt 8.1 och kan omfatta, men behöver inte begränsas till:

- Olika typer av användarklient ska ha IT-säkerhetsspecifikation för vilken typ av information och klassningsnivå som användarklienten kan hantera.
- Användarklienter ska vara registrerade.
- Användarklienter ska ha säker fjärrstyrd programinstallation.
- Användarklienter ska omfattas av krav på aktuella programversioner och automatisk uppdatering av betrodd programvara.
- Kryptering av lagringsenhet.
- Skydd mot skadlig kod.
- Säkerhetskopiering av personlig profil och data.
- Möjlighet att inaktivera eller låsa kontot från distans.
- Möjlighet att logga användning för analys av slutanvändares beteende.
- Möjlighet att centralt sätta regler och styra flyttbara enheter och portar.

9 Övervakning

Kontinuerlig automatiserad och manuell övervakning är en förutsättning för ett fungerande cybersäkerhetsarbete, säker drift och tillgänglighet av verksamhetskritiska IS/IT-tjänster samt för att nå upp till svensk lagstiftning och europeiska direktiv och förordningar. Syftet med en kontinuerlig övervakning är att säkerställa upptäckt av avvikande händelser, incidenter, sårbarheter och attacker i realtid. Loggning, övervakning, monitorering och skydd mot skadlig kod samverkar för att uppnå detta.

9.1 Loggning

Loggning för alla IS/IT-tjänster och informationsbehandlingsresurser ska utföras för att bevara

riktighet och möjliggöra spårbarhet i enlighet med aktuell informationsklassning.

Loggning avser informationsåtkomstloggning (exempelvis vem som tittat på en patientuppgift), systemåtkomstloggning (exempelvis när någon loggat in i ett system och varifrån), systemloggning (exempelvis felmeddelanden från systemet). Åtgärder ska säkerställa följsamhet till relevanta delar av ISO/IEC 27002, avsnitt 8.15.

Loggdata ska lagras på säkra och lämpligt skyddade lagringsenheter som skyddar mot obehörig åtkomst, ändring, borttagning eller manipulation. Loggar ska finnas åtkomliga centralt för att möjliggöra övervakning. Vid incidenter ska loggdata kunna analyseras för att fastställa händelseförlopp och potentiellt involverade aktörer.

Applikationer där informationsbehandling omfattas av patientdatalagen har en särställning i att åtkomst av patientdata på individnivå måste loggas enligt lag och att dessa loggar ska bevaras och kunna granskas regelbundet genom så kallad loggranskning.

Loggningen ska kontinuerligt utvärderas och anpassas.

9.2 Övervakning

Övervakning är avgörande för att upptäcka och reagera på obehörig eller skadlig aktivitet mot VGR:s informationsbehandlingsresurser. Dessa gäller för alla IT-system, lokala nätverk och informationsbehandlingsresurser som ägs eller administreras av VGR. Åtgärder ska säkerställa följsamhet till relevanta delar av ISO/IEC 27002, avsnitt 8.16.

Övervakningen ska vara proaktiv och kontinuerlig för att möjliggöra tidig upptäckt av ovanliga eller misstänkta händelser. I situationer där man inte har tid och råd att övervaka precis allt så

ska fokus ligga på delar av IT-miljö enligt planer för kontinuitetshantering av IT-miljö i första hand och enligt aktuell riskbedömning och identifierade men ej hanterade sårbarheter i andra hand.

Övervakningen ska omfatta, men inte begränsas till, loggar, konfigurationer, IS/IT-tjänster, nätverk, sårbarheter och användarbeteende. Övervakningsverktyg som används ska vara kapabla att identifiera avvikande händelser som intrångsförsök och andra potentiella hot. Ett dokumenterat och testat svars/responssystem ska vara på plats för att hantera de incidenter som upptäcks.

9.3 Monitorering

Monitoreringslösningar ska vara implementerade för att aktivt övervaka nätverkskomponenters mjuk- och hårdvarustatus. För att säkerställa adekvat tillgänglighet ska monitorering användas för att ge underlag för kapacitetsdimensionering.

9.4 Skydd mot skadlig kod

VGR:s klienter, servrar och nätverkskomponenter ska ha skydd mot skadlig kod. Åtgärder ska säkerställa följsamhet till relevanta delar av ISO/IEC 27002, avsnitt 8.7.

Åtgärder för skydd mot skadlig kod kan omfatta, men behöver inte vara begränsade till:

- Verktyg för upptäckt av användning av icke tillåten hård- eller mjukvara
- Verktyg för förhindrande av användning av icke tillåten hård- eller mjukvara
- Verktyg för upptäckt av användning av kända eller misstänkt skadliga webbplatser

- Verktyg för förhindrande av användning av kända eller misstänkt skadliga webbplatser
- Regelbundna automatiserade översyner av programvara efter icke godkända filer eller obehöriga ändringar.
- Regelbundna uppdateringar av program för upptäckt av skadlig kod och återställning
- Isolera miljöer med ökad risk för/av skadlig kod
- fastställa anvisningar och ansvar för hantering av skydd mot skadlig kod i system, inklusive användarutbildning, rapportering och återställning efter attacker orsakade av skadlig kod.

10 Immateriella rättigheter

VGR ska säkerställa efterlevnad av författningskrav och avtalskrav som rör immateriella rättigheter och användning av proprietära produkter vid utveckling av en tjänst och i en tjänst. Här avses de delar som rör mjukvara och mjukvarulicenser under utveckling.

Dokumentationen och dess tillämpning i utvecklingsuppdrag ska säkerställa följsamhet till lagstiftning och tillämpliga delar av avsnitt 5.32 i ISO/IEC 27002.

11 Hantering av tekniska sårbarheter

Tekniska sårbarheter övertas av ägare IS/IT-tjänst vid överlämning till drift och hanteras under hela livscykeln enligt *Hantering av sårbarheter i IT-miljö- Regional rutin 2025-2029*.

Relaterade dokument

- Informationssäkerhet och dataskydd - Regional riktlinje 2023–2027 (dnr RS 2023-02811)

- Informationsklassning - Regional rutin 2024 – 2028 (dokument-id: RS10162-1596316381-102)
- Riskhantering för informationssäkerhet - Regional rutin 2024 – 2028 (dokument-id: RS10162-1596316381-118)
- Säker utveckling - Informationssäkerhet och dataskydd vid verksamhetsutveckling - Regional rutin 2024–2028 (dokument-id: RS10162-1596316381-136)
- Kontinuitetshantering av IS/IT-tjänst- Regional rutin 2024-2028 (dokument-id: RS10162-1596316381-279)
- Hantering av sårbarheter i IT-miljö- Regional rutin 2025-2029 (dokument-id: RS10162-1596316381-332)
- Informationssäkerhet för extern molntjänst - Regional rutin 2024 – 2028 (dokument-id: RS10162-1596316381-126)
- Nätverkssäkerhet- Regional rutin 2024-2028 (dokument-id: RS10162-1596316381-346)
- IT-säkerhetsspecifikation- Regional rutin 2024-2028 (dokument-id: RS10162-1596316381-111)

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Jakob Sandberg, (jaksa4), Regionutvecklare

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-367

Version: 1.0

Giltig från: 2025-07-14

Giltig till: 2029-10-04