Gäller för: Västra Götalandsregionen
Innehållsansvar: Fredrika Holm Fredriksson, (freho10), Strateg
Godkänd av: Johan Flarup, (johfl), Direktör
Giltig från: 2025-05-07
Giltig till: 2029-12-31

Nätverkssäkerhet

Regional rutin 2025 – 2029

Ledningssystem för informationssäkerhet och dataskydd

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

Inledning

Mål: Nätverk och nätverkstjänster ska skyddas, hanteras och styras för att skydda information i system och applikationer samt för att säkerställa att nätverk och nätverkstjänster fungerar säkert och stabilt.

Säkerhetsåtgärder ska användas för att säkerställa en robust och säker nätverksinfrastruktur. Dessa skyddar datanätverk, informationsbehandlingsresurser och dataöverföring mot risker som kan innebära förstörande och/eller röjande av informationstillgångar, samt att möjliggöra en snabb återhämtningsförmåga vid en eventuell incident.

Denna rutin är styrande för alla förvaltningar och bolag i Västra Götalandsregionen och ingår i ledningssystemet för informationssäkerhet och dataskydd (LISD). Rutinen fastställer de tekniska säkerhetsåtgärder som ska användas för att upprätthålla säkra nätverkstjänster.

Rutinen riktar sig primärt till ägare IS/IT-tjänst samt övriga med uppgifter att hantera informationssäkerhet inom VGR:s nätverksmiljö.

Termer och begrepp

Termer och begrepp är bland annat hämtade från MSB termbank och standarden ISO 27002. Utöver dessa källor är det termer som förklarar VGR:s nätverksmiljö.

Term	Beskrivning
Datanätverk	Datanätverk i detta dokument avser den samlade funktionen av nätverkskomponenter; routrar, switchar, brandväggar, kablage och accesspunkter som möjliggör säker datatrafik mellan digitala informationsbehandlingsresurser oberoende av trådbunden, trådlös samt mobil kommunikation.
Informations-behandlingsresurs	Digital eller fysisk resurs för behandling av information. I dokumentet avses digital tjänst, system eller infrastruktur för informationsbehandling, till exempel nätverksresurs
IS/IT-tjänst	Är en avgränsning av en eller flera digitala informationsbehandlingsresurser. Exempelvis IT-system, applikation, mjukvara, nätverk, lagringssystem eller infrastruktur.
Nätverkskomponent	En enhet/utrustning, som utgör en installerad hårdvara med tillhörande mjukvara i nätverksinfrastrukturen med ändamålet att skapa kommunikation och styrning av datatrafik.
Nätverksmiljö	Avser i detta dokument VGRnet med dess perimeter. Omfattar den infrastruktur och dess komponenter som möjliggör kommunikation med och mellan IS/IT-tjänster. Säkerhetsåtgärder som avser nätverksmiljö omfattar produktions-, test- och utvecklingsmiljöer.
Nätverkstjänst	Avser bland annat av VGR tillhandahållna nätverksservicetjänster som DNS, DHCP, NTP och IPAM
Perimeter	Beskriver i dokumentet den omkrets eller upptagningsområde ett datanätverk begränsas av.
Portar	IS/IT-tjänster kommunicerar IP-datatrafik via anslutningar kallad port – kommunikationsport.
Protokoll (nätverk)	Avser här kommunikationsprotokoll, t.ex TCP/IP, för datatrafik. Regler mellan tjänster om hur man ska kommunicera över ett datanätverk.
VGRnet	VGR:s nätverksmiljö som omfattar produktions-, test- och utvecklingsnätverk (se nätverksmiljö)
Öppna gästnätverk	Avser tjänster i dokumentet som till exempel det logiskt separerade nätverket VGR Publikt.

1 Ansvar och roller

1.1 Digitaliseringsdirektör

Ansvarar för att leverera en stabil och säker IT-plattform som möter informationsägares behov av säkerhetskrav.

1.2 Informationsägare

Alla informationstillgångar ska ha en utpekad informationsägare under hela tillgångens livscykel. Informationsägaren ansvarar för att genomföra de grundläggande informationssäkerhets- och dataskyddsanalyserna:

1. Informationsklassning
2. Riskhantering
3. Tröskelanalys
4. Konsekvensbedömning

Dessa analyser identifierar vilka säkerhetsåtgärder och krav som en IS/IT-tjänst ställer på nätverkssäkerheten.

1.3 Ägare IS/IT-tjänst

Ansvarar för att implementera och livscykelhantera de dokumenterade, och av informationsägare, godkända säkerhetsåtgärder som beslutats användas för IS/IT-tjänst.

2 Säkerhetsåtgärder för robust nätverksinfrastruktur

2.1 Nätverkssäkerhet

Avser följsamhet till säkerhetsåtgärd 8.20 enligt SS-EN ISO/IEC 27002:2022 (sis.se)

Nätverkssäkerhet i VGR:s nätverksmiljö omfattar alla trådbundna och trådlösa nätverk. Risken för störningar i driften av VGR:s nätverksmiljö ska minimeras. Störningar kan uppkomma genom till exempel misstag, ont uppsåt eller extraordinära och svårförutsedda händelser.

För att uppnå en robust och säker nätverksmiljö ska endast av koncernstab digitalisering (KSD) godkända nätverkskomponenter tillåtas att installeras och användas i nätverksmiljön och endast behöriga enheter, samt användare, tillåtas att ansluta sig.

Åtkomst till nätinfrastruktur för konfiguration eller administration ska använda säkra metoder för autentisering och auktorisering.

Det ska säkerställas att endast de nätverkskomponenters tjänster, protokoll och portar som krävs för avsedd funktion ska vara aktiverade, övriga ska vara inaktiverade eller avinstallerade.

Datakommunikation över nätverket ska vara skyddad mot avlyssning, kapning eller modifiering. Ägare av IS/IT-tjänst ska tillse att kommunikation till och från sina informationsbehandlingsresurser, och som använder VGR:s nätverksmiljö, är krypterad enligt *Användning av kryptering-regional rutin 2025-2029*.

För att säkerställa en enhetlig tillämpning av säkerhetsåtgärder ska åtgärder vidtas som ökar samordning i hantering av säkerhetsfunktioner. Exempel på åtgärder som ska användas är standardtjänster och beredningsfunktioner för att underlätta beställning och införande av säkerhetsfunktioner.

Följande åtgärder ska användas och efterlevas, men inte vara begränsat till, för att säkra nätverksmiljön:

a) Endast behöriga enheter, samt användare, ska tillåtas att ansluta till nätverket. Varje enskild klient och användare som gör försök till anslutning mot nätverksmiljön, ska kontrolleras mot fördefinierade säkerhetsregler.

b) Fysisk och/eller logisk segmentering av organisationens applikationer och nätverksresurser ska, som en del av regionens säkerhetsarkitektur, användas för att skydda information och informationsbehandlingsresurser.

c) Access till nätverkskomponenter ska vara baserad på principen om minsta behörighet och strikt reglerad. Varje enskild användare som gör åtkomstförsök till nätverkskomponenter, ska kontrolleras mot fördefinierade åtkomst- och säkerhetsregler samt flerfaktorautentisering ska tillämpas.

d) All access till nätverkskomponenter, ska auditloggas.

e) Monitoreringslösningar ska vara implementerade för att aktivt övervaka nätverkskomponenters mjuk- och hårdvarustatus.

f) Övervakningslösningar ska vara implementerade för att aktivt övervaka nätverkstrafik och identifiera skadlig trafik och avvikande aktivitet.

g) Sårbarhetsanalyser ska genomföras med lämplig regelbundenhet (minst årligen).

h) Säkerhetshot och incidenter ska åtgärdas skyndsamt, bedömt utifrån klassning av känslighets- och viktighetsgrad samt utifrån eventuella andra påverkansfaktorer.

i) Loggning av nätverksaktiviteter, och analys av dessa loggar, ska genomföras för att upptäcka avvikelser.

j) Nätverkskomponenter ska vara uppdaterade med de senaste av tillverkaren rekommenderade, samt av VGR testade och godkända säkerhetsuppdateringarna.

k) Konfigurationer och data i nätverkskomponenter och nätverkstjänster ska säkerhetskopieras och versionshanteras.

l) Ansvar ska segregeras mellan de som sköter drift av datanätverk, från de som utvecklar/designar datanätverket.

m) Det ska säkerställas att aktiviteter som utförs på datanätverket som stödjer verksamhetskritiska tjänster inte är beroende av en enskild individ.

n) Behörigheter för hantering av nätverksmiljön ska kontrolleras och underhållas med en regelbundenhet som är dokumenterad.

2.1.1 Trådlösa nätverk

Trådlösa nätverk kan ha en otydlig perimeter och radiotrafik som sträcker sig mellan rum och utanför huskroppar eller hustomter. För att förhindra obehörig åtkomst och avlyssning till VGR:s trådlösa nätverk ska onödigt radioläckage minimeras genom att anpassa radiotäckning för dess ändamål.

Rutinens säkerhetsåtgärder ska användas för att skydda dessa trådlösa nätverk och att se till att skilja datatrafik med högt skyddsbehov från osäker datatrafik.

VGR:s trådlösa gästnätverk ska minst omfattas av samma begränsningar som trådlösa nätverk för personal, för att förhindra osäkert användande.

2.1.2 Externa nätverksmiljöer

Externa leverantörer som är avtalspartners med VGR kan vid extern drift leverera en IS/IT-tjänst med tillhörande nätverk som kan anses bli en del av den perimeter som omfattar VGR:s nätverksmiljö.

Kontroll och bedömning av dessa nätverk ska genomföras av koncernstab digitalisering för att säkerställa att adekvata säkerhetsåtgärder följs. Kontroll ska utföras vid upphandling och förändring av IS/IT-tjänst, samt genom avstämningar under avtalsperiod.

2.2 Säkerhet i nätverkstjänster

Avser säkerhetsåtgärd 8.21 enligt SS-EN ISO/IEC 27002:2022 (sis.se)

Med nätverkstjänster avses i denna rutin tjänster och komponenter som möjliggör anslutning till nätverket för klienter och IS/IT-tjänster samt driftlösningar för att hantera nätverkssäkerhet. Följande ska säkerställas:

- Nätverkstjänster som levereras av koncernstab digitalisering omfattas av de åtgärder som presenteras i kapitel 2.1.

- Levereras nätverkstjänst av extern leverantör, ska avtal vara upprättade med leverantören, alternativt tredjepartsintyg, som ska säkerställa att tjänstens skyddsnivå överensstämmer med VGR:s behov av skydd utifrån informationsklassning och riskhantering.

Ägare IS/IT-tjänst ansvarar för att kontroller och revisioner med externa leverantörer utförs enligt en överenskommen periodicitet för att tillse att säkerhetsåtgärder efterlevs.

2.3 Segmentering

Avser säkerhetsåtgärd 8.22 enligt SS-EN ISO/IEC 27002:2022 (sis.se)

Segmentering är en säkerhetsåtgärd som ser till att säkerställa att endast behörig kommunikation sker mellan IS/IT-tjänster, servrar och datorer. När segmentering används hindrar eller försvårar det en angripares rörelsemönster och det avgränsar till färre attackytor. Det medför mindre skadeverkan och möjlighet till enklare åtgärdshantering. Segmentering medför flera viktiga säkerhetsfunktioner:

- Hanterar likvärdigt klassad och riskbedömd information och resurser på ett enhetligt sätt.
- Underlättar hantering av tjänster med samma behov av tillgänglighet.
- Skyddar informationstillgångar från obehörig åtkomst och obehörigt röjande (kravet på konfidentialitet).

- Hindrar eller försvårar spridning av en cyberattack.
- Isolerar uppkomna incidenter till ett begränsat område.
- Medför enklare övervakning, upptäckt och hantering av sårbarheter och hot.
- Förbättrar prestanda.
- Bidrar till följsamhet med lagkrav, standarder och certifieringar.

Ägare IS/IT-tjänst ansvarar för att leverera segmentering utifrån informationsägarens krav. Informationsägaren godkänner åtkomst till information samt resurser. Anslutning som ger åtkomst mellan segment, ska godkännas av alla inblandade informationsägare eller av regional processägare.

Nätverkssegmentering ska användas för att dela upp ett datanätverk i separata delar. Varje del utgör ett eget nätverkssegment där kontakten med andra segment begränsas till endast vad som är nödvändigt.

Applikationssegmentering ska användas, men inte begränsas till, att isolera en applikation med ett högt skyddsbehov och även användas för att isolera applikationer som har en hög riskprofil, till exempel med osäkra mjukvaror och när det inte är möjligt att patcha, hantera eller verifiera uppdateringar på applikationer.

Segmentering ska genomföras med hjälp av fysisk eller logisk segmentering, eller en kombination av dessa. Fysisk segmentering innebär fysisk åtskillnad av applikation eller datanätverk där segmenten inte delar några nätverkskomponenter. Logisk segmentering hanteras med hjälp av tekniska åtgärder på ett och samma fysiska datanätverk och styrs av konfiguration i nätverkskomponenter som filtrerar trafiken mellan segmenten.

Det ska finnas tydlig definierad åtkomststyrning som hanterar kommunikation mellan segment. Användare och system i datanätverket ska endast ha tillgång till det som är nödvändigt för deras arbetsuppgifter. Penetrationstester och simuleringar ska genomföras för att testa och verifiera att segmentens åtkomststyrning fungerar som förväntat.

2.4 Webbfiltrering

Avser säkerhetsåtgärd 8.23 enligt SS-EN ISO/IEC 27002:2022 (sis.se)

Webbfiltrering syftar till att säkerställa att användarnas åtkomst till webbtrafik hanteras på ett säkert och ansvarsfullt sätt för att förhindra åtkomst till skadliga webbplatser och minska risken för attacker. Ägare IS/IT-tjänst ansvarar för att implementera säkerhetsåtgärden utifrån informationssäkerhetschefens krav.

Webbfiltreringslösning ska övervaka och reglera användarens webbaktiviteter och blockera åtkomst till skadliga webbplatser, domäner och dess innehåll. Vilken webbåtkomst som ska blockeras eller tillåtas ska fastställas, dokumenteras och på en lämplig nivå kommuniceras till användare. Följande ska tas hänsyn till:

- Webbfiltreringsregler ska vara implementerade som har följsamhet med VGR:s fastställda policys, riktlinjer och övriga aktuella regler och som ska skydda VGR:s användare och nätverksmiljö mot skadlig kod och olämpligt innehåll med mera.
- Loggning och övervakning av aktiviteter ska vara implementerade i webbfiltreringslösningen för att upptäcka eventuella avvikelser.
- Webbfiltreringens reglers effektivitet ska utvärderas med lämplig regelbundenhet och justeras efter behov.

3 Dokumentation

Koncernstab digitalisering ansvarar för att det finns uppdaterad dokumentation för att kunna underhålla nätverksinfrastruktur och nätverkstjänster på ett säkert och korrekt sätt. Det omfattar bland annat styrande rutiner och tillämpningsanvisningar som ska möjliggöra och skapa grund för en enhetlig och konsekvent nätverksmiljö med dess implementerade säkerhetsåtgärder.

Dokumentation som beskriver datanätverkets infrastruktur, nätverksresurser och övriga applikationer samt dess implementerade säkerhetsåtgärder ska informationsklassas och skyddas utifrån det behov av skydd som informationen har. Åtkomst till denna dokumentation ska begränsas till endast behöriga personer.

Ägare av IS/IT-tjänst ska dokumentera och versionshantera tjänsternas åtkomstregler, för att ha kontroll och möjliggöra uppföljning, interna revisioner och granskningar.

4 Relaterade dokument

1. Termbank för informationssäkerhet - nationell terminologi för informations- och cybersäkerhetsområdet https://termbanken.informationssakerhet.se/

- 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)
- Tröskelanalys avseende dataskydd – Regional rutin 2024-2028
- Konsekvensbedömning avseende dataskydd – Regional rutin 2024-2028
- Användning av kryptering - Regional rutin 2024-2028

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Fredrika Holm Fredriksson, (freho10), Strateg

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-346

Version: 1.0

Giltig från: 2025-05-07

Giltig till: 2029-12-31