Gäller för: Västra Götalandsregionen
Innehållsansvar: Fredrika Holm, (freho10), Strateg
Granskad av: Anders Falkeby, (andfa14), Avdelningschef
Godkänd av: Regionstyrelsen, (RS),

Giltig från: 2024-08-06
Giltig till: 2027-08-29

Informationssäkerhet och dataskydd

Regional riktlinje 2023 – 2027 (RS 2023–02811)
Ledningssystem för informationssäkerhet och dataskydd

VÄSTRA GÖTALANDSREGIONEN

1.Inledning

Ett ändamålsenligt informationssäkerhetsarbete är en skyldighet och en förutsättning för att kunna upprätthålla Västra Götalandsregionens (VGR:s) förmåga som en samhällsviktig aktör att nå sina verksamhetsmål samt vara en del av det civila försvaret. Det är även en förutsättning för en god patientsäkerhet, en kvalitativ och säker vård, en framgångsrik digitalisering samt ett ändamålsenligt skydd för den personliga integriteten för såväl invånare som medarbetare.

Ändamålsenlig informationssäkerhet och skydd för den personliga integriteten förutsätter ett strukturerat och systematiskt arbete som är integrerat i det dagliga arbetet i alla verksamheter som hanterar information. Genom ett samordnat arbete mellan verksamhet och IT samt andra stödfunktioner kan väl avvägda bedömningar för lämpliga säkerhetsåtgärder göras och en god och säker informationshantering uppnås.

Denna regionala riktlinje är styrande för alla förvaltningar och majoritetsägda bolag i VGR och ingår i ledningssystemet för informationssäkerhet och dataskydd (LISD). [1]Riktlinjen utgår från och konkretiserar policy för säkerhet och beredskap (RS 2018-00129) som beskriver regionens övergripande mål och inriktning för informationssäkerhets- och dataskyddsarbetet. Utöver riktlinjen finns tillhörande rutiner och stödjande material inom informationssäkerhet, dataskydd, cybersäkerhet och IT-säkerhet som beskriver hur arbetet inom området ska genomföras. Kompletterande styrande och stödjande dokument finns angivna i särskild förteckning.

1.1 Mål

Det övergripande målet för informationssäkerhet och skyddet för den personliga integriteten är *”**att rätt och riktig information ska nå rätt mottagare i rätt tid och vara skyddad från obehörig åtkomst och förstörelse samt att samhällsviktig verksamhet kan upprätthållas på ett säkert och robust sätt”.***

1.2 Omfattning

Riktlinjen är styrande för informationssäkerhets- och dataskyddsarbetet i VGR och gäller medarbetare, extern personal, förtroendevalda och andra

[1] När det i dokumentet anges verksamhet, myndighet eller förvaltning menas även bolag.

som ges tillgång till VGR:s informationstillgångar om inte annat anges i kompletterande regionala rutiner. Riktlinjen gäller även regionens avtalsparter där det i avtalet anges att VGR:s regelverk ska följas.

Med informationstillgång menas information och informationsbehandlande resurser som är av värde för en organisation. Informationstillgångar kan vara allt från applikationer, datorer, nätverk till människor eller immateriella tillgångar.[2]

1.3 Ledningssystem för informationssäkerhet och dataskydd (LISD)

Ledningssystemet för informationssäkerhet och dataskydd (förkortat LISD) är en del av verksamhetens ledningssystem. LISD inkluderar mål, styrdokument, organisation och processer för informationssäkerhet, dataskydd, cybersäkerhet och IT-säkerhet. Riktlinjen tar sin utgångspunkt i SS-ISO/IEC 27000-serie för informationssäkerhet och personlig integritet som en utgångspunkt för att bedriva ett systematisk och riskbaserat informationssäkerhetsarbete

1.3.1 Vad är informationssäkerhet och dataskydd?

Informationssäkerhet är skydd av informationstillgångar utifrån informationssäkerhetsperspektiven:

- **Konfidentialitet-** att informationstillgång inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer
- **Riktighet-** att informationstillgången skyddas mot oönskad förändring
- **Tillgänglighet-** att informationstillgång är åtkomlig och användbar inom förväntad tid och omfattning

Informationssäkerhet är teknikneutralt och omfattar skydd av såväl muntlig, pappersbunden som digital information. Cybersäkerhetsarbetet, som syftar till att skydda digitaliserade system mot antagonistiska hot, liksom IT-säkerhetsarbetet som är avgränsat till hot mot IT-resurser[3], är en del av informationssäkerhetsarbetet.

[2] Definition från MSB:s Termbank för informationssäkerhet
[3] För definition av cybersäkerhet och IT-säkerhet, se MSB:s termbank Termbank för informationssäkerhet

Dataskydd omfattar skydd för den personliga integriteten vid behandling av personuppgifter och är också det en del av informationssäkerhetsarbetet.

Skyddet av informationstillgångar ska vara väl avvägt utifrån det skyddsvärde som de har och de skyddsåtgärder som identifieras och införs ska anpassas utifrån hela hotskalan - från försumbar information till säkerhetsskyddade uppgifter som ska skyddas utifrån Sveriges säkerhet. Information som omfattas av säkerhetsskyddslagen omfattas av kraven i LISD men kompletteras av de särskilda krav som finns inom processerna för säkerhetsskydd.

2. Grundläggande principer för personuppgiftsbehandling

Vid behandling[4] av personuppgifter[5] ska de grundläggande principerna i dataskyddsförordningen följas. Principerna innebär att personuppgiftsansvarig[6]:

- måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter
- bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål
- inte ska behandla fler personuppgifter än vad som behövs för ändamålen
- ska se till att personuppgifterna är riktiga
- ska radera personuppgifterna när de inte längre behövs
- ska skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs
- ska kunna visa att och på vilket sätt dataskyddsförordningen efterlevs.

[4] Behandling är enligt dataskyddsförordningen: "en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.” (MSB:s termbank *Personuppgiftspolicy*)

[5] all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet (MSB:s termbank *Personuppgifter*)

[6] Varje nämnd och styrelse i Västra Götalandsregionen utgör personuppgiftsansvarig.

3. Ansvar och roller

Mål: Organisationen ska ha ett riskmedvetande och informationssäkerhetsarbetet ska vara organiserat så att det finns ett tydligt ansvar och följer ordinarie berednings- och beslutsprocesser. För att uppnå och bibehålla en god informationssäkerhet inom regionen ska ansvar definieras och tilldelas. Ansvaret sträcker sig från den politiska ledningen, genom tjänstemannaledningen till interna och externa medarbetare.

3.1 Övergripande ansvar

3.1.1 Regionfullmäktige

Regionfullmäktige är ytterst ansvarig för säkerhetsarbetet i VGR och beslutar om VGR:s säkerhets- och beredskapspolicy samt om långsiktiga mål för informationssäkerhetsarbetet.

3.1.2 Regionstyrelsen

Regionstyrelsen har genom sitt samordningsansvar ansvar för att en effektiv och ändamålsenlig organisation upprätthålls avseende informationssäkerhet och dataskydd och ansvarar för att ledningssystemet för informationssäkerhet och dataskydd uppnår sitt avsedda resultat. Regionstyrelsen ska säkerställa att de krav och säkerhetsåtgärder som rör ledningssystemet för informationssäkerhet och dataskydd är integrerat i organisationens processer.

3.1.3 Regiondirektören

Regiondirektören ansvarar på uppdrag av regionstyrelsen för att leda, samordna, granska och följa upp informationssäkerhets- och dataskyddsarbetet i regionen. Ansvaret innebär att regiondirektören har att verkställa de beslut som regionstyrelsen fattar och stödja regionstyrelsen i uppfyllandet av sitt ansvar för informationssäkerhet.

Regiondirektören ansvarar för att informationssäkerhets- och dataskyddsarbetet bedrivs effektivt så att målen inom informationssäkerhet och dataskydd uppnås. Regiondirektören beslutar om vem som företräder informationsägare för informationsbehandlingsresurser som är gemensamma i regionen.

3.1.4 Informationssäkerhetschef (CISO)

Informationssäkerhetschefen (CISO) ska leda, samordna, utveckla och följa upp informationssäkerhets- och dataskyddsarbetet, inklusive cybersäkerhets- och IT-säkerhetsarbetet, i VGR. Arbetet med informationssäkerhet och dataskydd är en delprocess i VGR:s samlade arbete med säkerhet och beredskap. Styrning och ledning av CISO:s uppdrag utgår från funktionsområde säkerhet- och beredskap.

I ansvaret ingår att förvalta ledningssystemet för informationssäkerhet och dataskydd, att ha ansvar för regionens kontakter med relevanta myndigheter och organisationer i informationssäkerhets- och dataskyddsfrågor, att ta fram och förvalta regiongemensamma utbildningar inom området samt att hålla samman nätverk och grupperingar inom området i organisationen.

3.2 Verksamhetsansvar

3.2.1 Styrelser, nämnder och bolagsstyrelse

Varje styrelse, nämnd och bolag ansvarar för informationssäkerheten och personuppgiftsbehandlingen som sker i egen verksamhet (är personuppgiftsansvarig) och har ansvar för att personuppgifter och annan information behandlas och skyddas på ett ändamålsenligt sätt och i enlighet med tillämpligt regelverk. För de fall nämnden eller styrelsen istället behandlar personuppgifter för annan organisation eller myndighets räkning (i egenskap av personuppgiftsbiträde) ansvarar denne för att sådan behandling sker i enlighet med de särskilda krav som gäller för personuppgiftsbiträden samt enligt instruktioner från den personuppgiftsansvarige organisationen.

Styrelsen, nämnden och bolaget ska följa upp sin verksamhet kontinuerligt och säkerställa att den får tillräcklig information för att kunna ta sitt ansvar för verksamheten.

Varje styrelse, nämnd och bolag ska utse ett dataskyddsombud.

3.2.2 Förvaltningschef/VD

Förvaltningschef/VD ansvarar för tillämpning av ledningssystemet för informationssäkerhet och dataskydd i den egna förvaltningen och tar vid behov fram kompletterande lokal styrning inom området. Förvaltningschefen/VD ska leda och stödja verksamheten för att bidra till ett verkningsfullt ledningssystem för informationssäkerhet och dataskydd. Förvaltningschef/VD ska även säkerställa tillgång till resurser

och säkerställa att dessa har tillräcklig kompetens för att bedriva ett systematiskt informationssäkerhets- och dataskyddsarbete.

3.2.3 Medarbetare

Varje medarbetare ansvarar för den information som denne hanterar och har ansvar att känna till ledningssystemet för informationssäkerhet och dataskydd. Medarbetare ska ha förståelse för värdet av informationen och varför den ska skyddas samt ha tillräcklig kompetens för att kunna utföra sina arbetsuppgifter på ett säkert sätt.

Medarbetare ansvarar för att anmäla misstänkta eller pågående incidenter för att förhindra eller minimera informationssäkerhets- eller dataskyddsincidentens effekt.

Vad som anges om medarbetare gäller även extern part som utför uppdrag för VGR:s räkning.

3.3 Särskilt utpekade ansvar och roller

3.3.1 Informationsägare

Alla informationstillgångar ska ha en informationsägare. Informationsägaren ansvarar för att säkerställa implementation och efterlevnad av säkerhetsåtgärder utifrån krav på skydd för informationstillgångarna.

Grundprincipen är att informationsägarskapet följer det ordinarie verksamhetsansvaret. Detta gäller från ledning till enskilda medarbetare. Informationsägarskapet sammanfaller med ansvaret i verksamheten, till exempel ansvarar en avdelningschef för information inom avdelningen, eller en processägare för informationen inom processen. Den som anlitar entreprenör, inhyrd personal, konsulter eller leverantörer ska se till att dessa externa medarbetare i tillämpliga delar följer ledningssystemet för informationssäkerhet och dataskydd.

När informationstillgångarna ingår i regiongemensamma processer, regiongemensamma IS/IT- tjänster, projekt och/eller upphandlingar företräds flera myndigheters informationsägare av en regional processägare. Fördelning av processansvar följer av VGR:s processmodell (dnr nr RS 2022-05853).

3.3.2 Ägare av IS/IT-tjänst

Ägare av IS/IT-tjänst har ansvar för att, utifrån de krav som ställs på tjänsten genom informationsklassningen och utifrån de risker som

identifierats, att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder i IS/IT-tjänsten så att adekvat skydd uppnås i tjänsten.

3.3.3 Digitaliseringsdirektör

Digitaliseringsdirektören ansvarar för att utifrån informationsägarens krav på skydd leverera en stabil och säker IT-plattform med ändamålsenliga IS/IT-tjänster samt identifiera, skydda, upptäcka, hantera och återställa VGR:s IT-miljö mot säkerhetshot.

3.3.4 Koncerninköpschef eller annan med motsvarande mandat

Koncerninköpschefen eller annan med motsvarande mandat ansvarar för att den information som hanteras under upphandlingsarbetet behandlas på ett säkert sätt både inom VGR och hos intresserade leverantörer samt att varan eller tjänsten uppfyller de krav på informationssäkerhet och dataskydd som identifierats som nödvändiga vid tecknande av avtal/anskaffning/inköp.

3.3.5 Ansvar i projekt

Informationssäkerhetsarbetet ska vara en integrerad del i projekt. Projektägaren ansvarar för att informationssäkerhetsarbete genomförs i projektet. Detta gäller alla typer av projekt oavsett komplexitet, omfattning, varaktighet, ämnesområde eller tillämpningsområde.

Projektägaren ska i ett tidigt skede identifiera vem som är regional processägare eller informationsägare och som kan fatta beslut om informationen och dess säkerhet såväl under projektet som efter projektets avslut. Då projektet avslutas och övergår i ordinarie förvaltning är det regional processägare alternativt informationsägare som övertar ansvaret för att säkerställa skyddet av informationen och det löpande arbetet med identifierade informationssäkerhetsrisker.

3.3.6 Ansvar i samverkan

I samverkan med andra aktörer utanför organisationen ska informationsägarskap och personuppgiftsansvar identifieras och dokumenteras.

3.3.7 Informationssäkerhetsamordnare

Informationssäkerhetssamordnaren är ett stöd till verksamheten i dess informationssäkerhetsarbete och verkar för en regiongemensam tillämpning av interna styrdokument och regelverk i den egna

verksamheten. Varje förvaltning ska ha en utsedd informationssäkerhetssamordnare.[7]

3.3.8 Dataskyddssamordnare

Dataskyddssamordnaren är ett stöd till verksamheten i dess dataskyddsarbete och verkar för en regiongemensam tillämpning av interna styrdokument och regelverk i den egna verksamheten. Varje förvaltning ska ha en utsedd dataskyddsamordnare.

3.3.9 Dataskyddsombud

Varje personuppgiftsansvarig ska ha ett dataskyddsombud.

Dataskyddsombudet övervakar att verksamheten följer dataskyddsförordningen och är kontaktperson gentemot tillsynsmyndigheten.

4. Hantering av informationstillgångar

Mål: Verksamheten ska identifiera vilken information och andra relaterade informationstillgångar som finns och fastställa dess betydelse för verksamheten. Informationsbehandlingsresurser ska klassas och skyddas på rätt sätt.

4.1 Ansvar för tillgångar

För information och informationstillgångar ska ägarskap tilldelas.

En förteckning över information och relaterade tillgångar ska upprättas och underhållas med syftet att identifiera verksamhetens information för att bevara informationssäkerheten och tydliggöra ägarskap.

Regler för tillåten användning av information och relaterade tillgångar ska identifieras, dokumenteras och införas av den som äger tillgången. Användare ska göras medvetna om de krav på informationssäkerhet som gäller för tillgångarna.

Tillgångar ska återlämnas då anställning, uppdrag eller avtal upphör.

[7] Informationssäkerhetssamordnarens och dataskyddssamordnarens uppgifter definieras mer ingående i kompletterande styrande och stödjande dokument som finns angivna i särskild förteckning.

4.2 Informationsklassning

Informationsklassning är en grundläggande aktivitet i det systematiska informationssäkerhetsarbetet. Informationsklassning innebär att verksamhetens information värderas utifrån vilka konsekvenser ett otillräckligt skydd för informationens konfidentialitet, riktighet och tillgänglighet skulle kunna få. Klassningsresultatet utgör underlag för att välja ändamålsenliga säkerhetsåtgärder.

Informationsägaren ansvarar för att informationsklassning görs.

4.3 Hantering av informationstillgångar vid lagring och överföring

Säkerheten för informationen som ska överföras inom organisationen eller till andra aktörer ska upprätthållas och dokumenteras.

När arbete utförs på distans ska informationssäkerheten vara säkerställd för att skydda information som nås, bearbetas eller lagras utanför organisationens lokaler.

4.4 Tillgängliggörande av information

För att kunna tillgängliggöra information, exempelvis såsom öppen data, måste informationssäkerheten för det som ska publiceras säkerställas. Informationen som tillgängliggörs ska vara informationsklassad och riskhanterad för att identifiera konsekvenser av ett otillräckligt skydd vid och under tillgängliggörandet för den personliga integriteten, för verksamheten eller för Sveriges säkerhet. Informationsägaren ska säkerställa att säkerhetsåtgärder kring tillgängliggörandet anpassas efter eventuella förändringar i behov, användningsområden och teknisk utveckling.

5. Riskhantering

Mål: Informationssäkerhetsrisker som kan påverka VGR:s informationssäkerhetstillgångar och de registrerades integritet ska identifieras, analyseras, behandlas och följas upp.

Riskhantering är samordnade aktiviteter för att styra och leda en organisation med avseende på risk. Riskhanteringsprocessen i VGR är en generisk modell, som ska tillämpas av varje verksamhet och vara en del av beslutsunderlaget inför förändringar.

Ansvar för riskhanteringen följer ansvaret för informationstillgången.

5.1 Behandling av personuppgifter som kan leda till hög risk

Om en behandling av personuppgifter sannolikt leder till hög risk för de registrerades fri- och rättigheter ska en konsekvensbedömning göras.

6. Åtkomst till informationstillgångar

Mål: Användare ska ha tillgång till rätt information på rätt sätt för sin arbetsuppgift och vara medveten om sitt personliga ansvar.

All åtkomst ska styras så att endast behöriga får tillgång till informationstillgångar.

Informationsägaren beslutar om behörigheter och ansvarar för en säker användning av behörigheter inom sin verksamhet. Det innebär att informationsägaren även beslutar om avslut av behörigheter. Behörigheter ska livscykelhanteras och ska baseras på aktuella arbetsuppgifter och organisatorisk tillhörighet. Varje användares digitala identitet ska kunna verifieras och alltid vara spårbar till en fysisk person. Ansvar för andra digitala identiteter ska också vara utsett och dokumenterat. För att kunna säkerställa korrekt användning av behörigheter behöver i vissa fall loggning och uppföljning genomföras. Informationsägaren beslutar om vilka säkerhetsåtgärder som krävs för åtkomst till informationstillgångar baserat på genomförd informationsklassning och riskbedömning.

Priviligierade åtkomsträttigheter ska tilldelas restriktivt och ställer högre krav på exempelvis loggning och uppföljning.

Åtkomst för IS/IT-tjänster till VGR:s IT-miljö kan i vissa fall stängas av då användningen utgör en risk för VGR. Mandat följer av utpekat verkställighetsansvar.

7. Personrelaterad säkerhet

Mål: Informationssäkerhetsåtgärder ska vara en del av anställningsprocessen och stå i proportion till verksamhetens krav, klassning av information som den anställde ska ges behörighet till och de risker som kan förekomma.

Innan anställning ska VGR pröva att individen bedöms lämplig för att hantera de för tjänsten aktuella informationstillgångarna. Vid rekrytering eller befordran till känslig eller särskilt informationssäkerhetskritiska arbetsuppgifter, ska flera och mer detaljerade bakgrundskontroller och referenstagning utföras.

All personal ska göras medvetna om sina skyldigheter vid hantering av VGR:s information samt om gällande regler för informationssäkerhet och sekretess. Ansvar för informationssäkerheten ska dokumenteras.

Anställda ska få utbildning i informationssäkerhet och dataskydd utifrån vad som är relevant för medarbetarens arbetsuppgifter. Lämplig kunskapsnivå ska bibehållas under medarbetarens hela anställnings- eller uppdragstid. Vid avslut av anställning eller uppdrag ska informationstillgångar återlämnas. Anställda ska skriftligen informeras om när fortsatt tystnadsplikt gäller.

Disciplinära åtgärder kan komma att vidtas när anställda brutit mot gällande ledningssystem för informationssäkerhet och dataskydd.

8. Informationssäkerhet i leverantörsrelationer

Mål: VGR:s informationstillgångar ska skyddas på ett likvärdigt sätt när tillgången hanteras av en extern leverantör.

Informationssäkerhetsrisker som förknippas med användningen av leverantörens produkter och tjänster ska hanteras.

Informationsägare eller dess företrädare ansvarar för att identifiera krav på informationssäkerhet och dataskydd som ska ställas på leverantör samt att granska leverantörens lämplighet utifrån relevanta krav. De informationssäkerhetskrav som gäller för en leverantör ska regleras i avtal och dess efterlevnad ska regelbundet följas upp.

Förändringar av tjänst eller produkt som kan ha påverkan på leverantörsavtal samt dess efterlevnad ska regelbundet följas upp.

Motsvarande informationssäkerhetskrav ska ställas på externa leverantörer som om VGR hade tillhandahållit IT-tjänsten i egen regi.

9. Fysisk och miljörelaterad säkerhet

Mål: VGR:s information samt informationstillgångar, som exempelvis lokaler och den utrustning som används för informationshantering, ska ha ett fysiskt skydd, skalskydd och tillträdeskontroll samt skydd mot angrepp, olyckor och naturkatastrofer på en nivå som identifierats genom informationsklassning och riskhantering.

Den som ansvarar för information och informationsbehandlingsresurs [8]ska säkerställa tillräckligt fysiskt skydd som identifierats genom informationsklassning och riskhantering. Högre krav ställs på information och informationsbehandlingsresurser som hanteras inom samhällsviktig verksamhet.

Kraven på fysisk säkerhet ska tillämpas för alla lokaler där information hanteras, samt för all utrustning som används för informationshantering. Information och utrustning ska skyddas på ett likvärdigt sätt oavsett om den hanteras innanför eller utanför organisation lokaler.

Utrymmen som innehåller informationstillgångar ska skyddas genom åtgärder som säkerställer att endast behöriga får tillträde till tillgångarna.

Utrustning som innehåller lagringsmedier bör granskas för att säkerställa att all känslig information och licensierade program har avlägsnats eller överskrivits på ett säkert sätt före avveckling eller före återanvändning.

[8] Med informationsbehandlingsresurs menas enligt MSB:s Termbank för informationssäkerhet en digital eller fysisk resurs för behandling av information, såsom IT-system eller infrastruktur men kan även vara en människa eller ett säkerhetsskåp.

10. Nätverks- och systemsäkerhet

Mål: Kommunikation och drift av IT-miljö, system och tillhörande informationsbehandlingsresurser ska ske utifrån fastställda rutiner för gemensam infrastruktur och de specifika säkerhetskrav som ställs genom verksamhetens informationsklassning.

10.1 Säkerhet i driftmiljön

VGR:s verksamhet bygger på informationshantering i ett stort antal system, tjänster och informationsbehandlingsresurser. För att få rätt nivå på säkerhet i denna helhet krävs tydlig ansvarsfördelning, eftersom säkerhetskraven från informationsägaren eller dess företrädare ska tas om hand av olika system- och resursägare.

Samtliga anslutningar till VGR:s interna IT-miljö ska vara godkända och dokumenterade.

Endast godkända applikationer ska vara aktiverade och möjliga att använda i organisationens IT-miljö. Alla applikationer ska förvaltas av utsedd ansvarig som säkerställer livscykelhantering och distribution av säkra versioner.

För att upprätthålla säker och tillförlitlig tillgång till information ska administration kring drift, övervakning och underhåll av VGR:s IS/IT-tjänster ske på ett strukturerat och systematiskt sätt enligt en tydlig ansvarsfördelning. Informationsbehandlingsresurser och den information som hanteras ska klassas och skyddas utifrån det behov av skydd som identifierats. Vilka säkerhetsåtgärder som har implementerats ska finnas dokumenterade. Information och informationsbehandlingsresurser ska skyddas på ett likvärdigt sätt, oavsett om den hanteras innanför eller utanför VGR:s lokaler eller IT-miljö.

Interna och externa sårbarhets- och penetrationstester ska genomföras, i syfte att verifiera att säkerhetsåtgärderna har förväntad effekt. Det ska finnas processer som säkerställer att system- och driftdokumentation är aktuell. Känslig dokumentation ska endast vara tillgänglig för behörig personal. VGR ska skyddas från förlust av data genom säkerhetskopiering

Inom VGR ska det finnas rutiner för att upptäcka och förhindra skadlig kod samt metoder för att återställa IS/IT-tjänsten efter angrepp av skadlig kod.

Loggning och övervakning ska tillämpas för att upptäcka och hantera sårbarheter som kan påverka informationssäkerheten samt ska ge

förutsättning för att händelsekedjor kan återskapas vid misstanke om brott. Loggar ska skyddas mot radering, manipulation och obehörig åtkomst. I övervakningsansvaret ingår sårbarhetsscanning, scanning av skadlig kod, kontroll av accesspunkter, kontinuerlig kontroll av administratörsrättigheter, genomlysning och rapportering av konton som inte kan associeras med en ägare eller verksamhetsprocess.

Funktioner och tjänster i driftmiljön som inte används ska avinstalleras eller avaktiveras. När IT-utrustning utrangeras, kasseras, säljs eller på annat sätt lämnar VGR ska det finnas instruktioner och rutiner för avinstallation och radering av information.

10.2 Nätverkssäkerhet

Säkerhetsåtgärder ska vara införda för att skydda överföring av information genom användning av alla typer av kommunikationsmedel. Organisationens datakommunikation ska skyddas i enlighet med informationsklassning och riskanalys. Patientdata eller annan känslig information ska skyddas genom kryptering.

Vid kommunikation över öppna nätverk ska särskilda skyddsåtgärder vidtas för att garantera konfidentialitet och riktighet för data som överförs. Alla anslutningar till VGR:s nätverk ska vara dokumenterade och godkända.

Egna enheter får endast användas då informationssäkerheten för VGR:s information kan säkerställas.

Enheter, såsom datorer eller terminaler för besökare, patienter eller liknande, ska vara skilda från kärnverksamhetens nätverk.

11. Anskaffning, utveckling och ändring av IS/IT-tjänster

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

Vid anskaffning, utveckling och ändring av IS/IT-tjänster ska säkerhetsåtgärder identifieras, specificeras och godkännas genom informationsklassning och riskhantering. Lämpliga säkerhetsåtgärder ska införas, förvaltas och utvärderas så att adekvat skydd uppnås i IS/IT-tjänsten. Säkerhetsåtgärderna ska vara dokumenterade.

Tester ska utföras för att säkerställa att IS/IT-tjänsten motsvarar kravställning och kan driftsättas, underhållas och inte medför skada på IT-miljön i VGR.

Det ska finnas en återställningsplan, som ska kunna användas i händelse av en misslyckad förändring i driftmiljö. Återställningsplanen ska vara en del av IS/IT-tjänstens kontinuitetsplan.

Vid anskaffning, utveckling, användning och avveckling av IS/IT-tjänster samt framtagande av rutiner ska hänsyn tas till principerna för behandling av personuppgifter. Genom förvalda inställningar i IS/IT-tjänster och beslutade arbetssätt ska verksamheten säkerställa att inte fler personuppgifter än nödvändigt samlas in, delas ut eller visas.

12. Hantering av informationssäkerhets- och personuppgiftsincidenter

Mål: Process, organisation och resurser ska finnas för att hantera incidenter på ett effektivt sätt.

VGR ska ha rutiner för att bedöma om informationssäkerhetshändelser ska kategoriseras som informationssäkerhetsincident och/eller personuppgiftsincident och ha en effektiv hantering av de incidenter som inträffar.

Informationssäkerhets- och personuppgiftsincidenter ska rapporteras, dokumenteras, eskaleras och följas upp inom respektive styrelse, nämnd och bolag. Incidenter som berör fler verksamheter eller som är av allvarligare karaktär ska rapporteras till Informationssäkerhetschefen (CISO) och ska samordnas regionalt.

Vid incidenter ska insamling och bevarande av bevis hanteras på ett verkningsfullt sätt med avseende på disciplinära och rättsliga åtgärder.

VGR ska på ett strukturerat sätt proaktivt förebygga att informationssäkerhets- eller personuppgiftsincidenter inte inträffar. Lärdomar ska dras av inträffade incidenter för att stärka och förbättra säkerhetsåtgärderna. Uppföljning ska ske såväl inom den egna myndigheten som på regional nivå till högsta ledning.

13. Kontinuitetshantering ur informationssäkerhetsynpunkt

Mål: Det ska finnas kontinuitetshantering för att säkerställa tillgång till information, IT-tjänster och funktioner som krävs för att upprätthålla av ledningen prioriterad verksamhet. Planeringen ska regelbundet testas och uppdateras.

Informationssäkerhetskrav ska vara en integrerad del av den övergripande kontinuitetshanteringsprocessen.[9]

Ansvarig för verksamhetsprocessen ansvarar för att identifiera vilka informationstillgångar som krävs för att de verksamhetskritiska processerna ska fungera som avsett samt att definiera krav på återställningstid samt maximal toleranstid för förlust av data vid ett avbrott. Vid höga tillgänglighetskrav behövs redundanta enheter eller redundant arkitektur. Även beroenden till nyckelpersoner för att upprätthålla verksamheten ska identifieras och dokumenteras i detta arbete.

Kravspecifikationen från verksamhet utgör underlag för vilka kontinuitetslösningar som väljs, hur reservrutiner ska utformas i verksamheten vid avsaknad av kritiska funktioner och informationstillgångar samt hur återgång till normalläge ska ske. Planer kan vara gemensamma för flera verksamheter och flera system och ska innehålla fastställda prioriteringsordningar för återgång till normalläge. Ägare av IS/IT-tjänst ansvarar för att upprätta en avbrotts- och återställningsplan för IS/IT-tjänsten, som tar sin utgångspunkt ifrån verksamhetens prioritering och informationsklassning.

Kontinuitetshanteringen ska fortlöpande stämmas av med verksamhetens beredskapsplan, för att säkerställa att dessa fungerar effektivt tillsammans samt regelbundet testas och uppdateras för att säkerställa att kontinuitetshanteringen är ändamålsenlig.

[9] Regional riktlinje för kontinuitetshantering 2023–2027-säkerställande av kritisk verksamhet vid störning

14.Uppföljning

Mål: Informationssäkerheten och informationssäkerhetsarbetet ska, som en del av den ordinarie verksamhetsredovisningen, regelbundet följas upp på central nivå och inom respektive nämnd, styrelse och bolag.

14.1 Kontroll av ändamålsenligt LISD

Informationssäkerhetschefen (CISO) ansvarar för att årligen följa upp verkan av det övergripande ledningssystemet för informationssäkerhet och dataskydd inom VGR och att årligen genom ledningens genomgång[10] rapportera detta till regionstyrelsen.

Baserat på genomförda granskningar och identifierade avvikelser ansvarar CISO för att åtgärder vidtas, anpassas och kompletteras för att säkerställa verkan av det övergripande LISDet. Uppföljningen ska ligga till grund för det ständiga förbättringsarbetet med ett ändamålsenligt LISD.

Informationssäkerheten och dess implementering bör med jämna mellanrum eller när betydande förändringar sker genomgå oberoende granskning.

14.2 Uppföljning av efterlevnad av LISD

Varje styrelse, nämnd eller bolag ska årligen följa upp informationssäkerheten och verkan av det övergripande ledningssystemet inom den egna myndigheten. Informationssäkerhet bör ingå som ett område i ledningens årliga säkerhetsredovisning och verksamhetens interna kontroll.

Baserat på genomförda granskningar och identifierade avvikelser ansvarar styrelsen, nämnden eller bolaget för att säkerhetsåtgärder vidtas, anpassas och kompletteras. Uppföljningen ska ligga till grund för det ständiga förbättringsarbetet med säker informationshantering.

[10] Metod för att systematisera kontakten med ledningen, se närmare Ledningens genomgang (informationssakerhet.se)

15. Avsteg

Om riktlinjen med dess kompletterande rutiner inte kan följas ska avstegsprocessen[11] följas.

[11] Se kompletterande styrande och stödjande dokument i särskild förteckning

Relaterade dokument

- Policy Säkerhet och beredskap i Västra Götalandsregionen (RS 2018-00129)
- Kompletterande styrande och stödjande dokument (samlas i särskild förteckning)
- Regional riktlinje för kontinuitetshantering 2023-2027- säkerställande av kritisk verksamhet vid störning (2023-01-26)
- VGR:s processmodell (RS 2022-05853)
- Säkerhetsåtgärder i svensk standard SS-ISO/IEC 27002:2022
- Termbank för informationssäkerhet - nationella terminologi för informations- och cybersäkerhetsområdet

Information om handlingen

Handlingstyp: Riktlinje

Gäller för: Västra Götalandsregionen

Innehållsansvar: Fredrika Holm, (freho10), Strateg

Granskad av: Anders Falkeby, (andfa14), Avdelningschef

Godkänd av: Regionstyrelsen, (RS),

Dokument-ID: RS10162-1596316381-117

Version: 6.0

Giltig från: 2024-08-06

Giltig till: 2027-08-29