Rutin

Gäller för: Västra Götalandsregionen
Innehållsansvar: Irja Burhöi, (irjbu1), Regionutvecklare
Godkänd av: Ann-Charlotte Lilja Järnström, (ancja6), Regiondirektör

Giltig från: 2025-12-28
Giltig till: 2029-12-31

Säkert beteende vid hantering av information

Regional rutin 2025-2029

Ledningssystem för informationssäkerhet och dataskydd

VÄSTRA GÖTALANDSREGIONEN

Innehåll

1. Inledning

Mål*: Information och andra relaterade tillgångar skyddas, används och hanteras på ett säkert sätt både inom och utanför Västra Götalandsregionens lokaler*.

Medarbetare inom Västra Götalandsregionen (VGR) hanterar dagligen information som är viktig för verksamheten och invånare, exempelvis patientuppgifter eller ekonomisk information. Information kan hanteras muntligen, i fysisk form och elektroniskt i olika IS/IT-tjänster och IT-utrustning, antingen inom VGR:s lokaler eller på distans. Medarbetaren ansvarar för sin hantering av information oavsett om den är digital, fysisk (som på papper) eller muntlig. Det är därför viktigt att alla medarbetare känner till hur information ska användas och får förutsättningar att hantera informationen säkert.

Syftet med rutinen är att tydliggöra hur information och informationstillgångar ska hanteras och motverka ett riskfyllt beteende. Rutinen tydliggör det ansvar medarbetare har för hantering av information, samt det ansvar övriga roller har för att ge medarbetaren rätt förutsättningar att efterleva sitt ansvar.

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

2. Termer och begrepp

Flyttbara lagringsmedium	En fysisk enhet som används för att lagra data permanent eller tillfälligt, exempelvis USB-sticka, CD-skiva, DVD-skiva, hårddiskar, med mera.
Informationstillgångar	Information och informationsbehandlande resurser som är av värde för en organisation.
Informationsägare	Grundprincipen är att informationsägarskapet följer det ordinarie verksamhetsansvaret. 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).
Informationsöverföring	Information som förs över antingen till en annan verksamhet/funktion/sammanhang inom Västra Götalandsregionen eller till en extern part. Informationsöverföring kan ske elektroniskt genom integrationer mellan olika system, via flyttbara lagringsmedier innehållande digital information, fysisk överlämning eller muntligt. Oavsett överföringsmetod ska informationen vid överföring skyddas i enlighet med den berörda informationens klassning.
IS/IT-tjänst	Är en avgränsning av en eller flera digitala informationsbehandlingsresurser. Exempelvis IT-system, applikation, mjukvara, nätverk, lagringssystem eller infrastruktur.

IT-utrustning	Fysiska enheter som används för att hantera information, exempelvis dator, mobiltelefon, USB-sticka, digitala mätinstrument, specialistutrustning, med mera.
Sekretessbelagd, känslig eller konfidentiell information	Information som inte får tillgängliggöras eller avslöjas för obehöriga individer, objekt eller processer. Vad som är sekretessbelagd information anges i offentlighets- och sekretesslagen. En del information kan vara känslig eller konfidentiell utan att omfattas av sekretess.

3. Tillåten användning av informationstillgångar

Medarbetaren, det vill säga alla som är anställda av VGR samt personer som utför arbete i VGR:s namn så som inhyrd personal, praktikanter och så vidare, får endast hantera den information som den har getts behörighet till på angivet sätt och för angivet ändamål.

IS/IT-tjänster och IT-utrusning som tillhandahålls av VGR är arbetsredskap och endast avsedda för arbetsrelaterade uppgifter[1].

3.1 Regler för användning av information

Informationsägaren ansvarar för att ta fram rutin för hur information ska hanteras vid olika arbetsmoment inom dennes ansvarsområde om regionala rutiner saknas. Rutinen ska följa lagkrav och VGR:s styrande dokument. Rutin för användning ska utgå ifrån informationens behov av säkerhetsåtgärder som identifierats i informationssäkerhetsanalysarbetet enligt LISD.

Rutinen ska informera medarbetare om vad som ska göras, när och hur samt med vilken IS/IT-tjänst och/eller IT-utrustning. Rutinen behöver vara tillräckligt detaljerad för att stötta medarbetaren i frågeställningar som kan uppstå vid informationshanteringen, exempelvis om och hur informationsöverföring ska gå till, vart information ska lagras, om kopior får skapas och hur de i så fall ska hanteras, eller om IT-utrustning behöver hanteras på något särskilt sätt.

Informationsägaren ansvarar för att endast hänvisa till godkända IS/IT-tjänster och IT-utrustning.

Medarbetaren ska följa framtagna rutiner om vad, när, hur och vart information får hanteras. Om det saknas rutiner, ska

[1] För närvarande finns möjlighet för anställda att använda mobiltelefon i rimlig omfattning för privat bruk om ansvarig chef medger detta och om avdrag på lönen görs varje månad.

medarbetaren fråga närmsta chef om hur informationen ska hanteras.

3.2 Säkerhetsmedvetet beteende

Samtliga medarbetare i VGR förväntas vara aktiva i arbetet med informationssäkerhet genom att exempelvis:

- Skydda sina inloggningsuppgifter och autentiseringsinformation och inte låna ut eller dela med sig av dessa till någon annan[2].
- Låsa dator och annan utrustning med skärmlås när den inte används eller lämnas obevakad.
- Vara uppmärksam på länkar, bilagor och QR-koder och anmäla misstänkta länkar och mejl.
- Använda olika lösenord till olika IS/IT-tjänster om dessa kräver egna lösenord samt använda starka lösenord i enlighet med VGR:s rekommendationer[3].
- Hämta utskrifter direkt eller använda sig av skrivare med autentiseringsfunktion (så kallad säker utskrift) så att inte obehörig får del av informationen.
- Inte släppa in obehöriga i VGR:s lokaler och bara ge behöriga åtkomst till VGR:s utrustning.
- Inte använda VGR:s e-post-verktyg för privat bruk.
- Rapportera in avvikelser och incidenter enligt rutin för incidenthantering.

3.3 Säkerhetsmedvetet beteende vid hantering av sekretessbelagd, känslig och konfidentiell information

Inom den offentliga sektorn är sekretess för de anställda reglerat i lag. Anställda kan inte avkrävas någon tystnadsplikt utöver vad

[2] Se punkt 1-4 under avsnitt 3.2 i rutin Åtkomst till information och relaterade tillgångar
[3] Se punkt 8 under avsnitt 3.2 i rutin Åtkomst till information och relaterade tillgångar

som anges i offentlighets- och sekretesslagen (SFS 2009:400) samt yttrandefrihetsgrundlagen (SFS 1991:1469).

Även information som inte omfattas av sekretess kan i vissa situationer bedömas som känslig eller konfidentiell och ska då hanteras med varsamhet.

Medarbetaren förväntas vara aktiv i att säkerställa att känslig, konfidentiell och sekretessbelagd information hanteras på ett säkert sätt genom att exempelvis:

- Ta lämpliga rumsliga säkerhetsåtgärder så som att säkerställa att skärmar inte visar sekretessbelagd, känslig eller konfidentiell information för obehöriga, exempelvis skärmens placering eller användande av skärmskydd.
- Vid samtal ta lämpliga rumsliga säkerhetsåtgärder så som att stänga dörr och fönster och vara i ett rum som är tillräckligt ljudisolerat för det samtalet rör.
- Vid samtal försäkra sig om att den som deltar i samtalet har rätt att ta del av informationen samt bör börja samtalet med att tillkännage att informationen de kommer höra är sekretessbelagd, känslig, eller konfidentiell.
- Vid digitala samtal använda sig av säkra kommunikationskanaler enligt informationsägarens anvisningar.
- Inte lämna meddelanden som innehåller sekretessbelagd, känslig eller konfidentiell information som röstmeddelande.
- Ta bort känslig information från white-board eller andra typer av displayer när den inte längre behövs.
- Låsa in sekretessbelagd, känslig eller kritisk verksamhetsinformation som finns i fysiskt format (exempelvis papper eller lagringsmedier) i dokumentskåp, kassaskåp eller annan säker förvaringsmöbel när den inte används.

3.4 Hantering av information utanför regionens lokaler och på allmänna platser

Vid arbete på distans ska medarbetaren följa rutin för distansarbete inom Västra Götalandsregionen.

Samma säkerhetsåtgärder som på arbetsplatsen gäller vid distansarbete men medarbetaren behöver även säkerställa att:

- Undvika uppkoppling mot offentliga nätverk.
- Uppkoppling av arbetsutrustning inte sker på osäkra nätverk.
- Vid uppkoppling mot öppna eller privata nätverk utanför Sverige ska VPN användas.
- Vid arbete med sekretessbelagd, känslig eller konfidentiell information ska ingen obehörig kunna ta del av informationen, varken övriga i hushållet/omgivningen, via insyn utifrån, via övervakning/säkerhetskameror, eller likande. Om det är lyhört där arbetet sker, tänk på att inte prata om sekretessbelagd eller känslig information.
- Vid arbete under resa med allmänna färdmedel eller på offentliga platser ska informationen skyddas så den inte är synlig för obehöriga, exempelvis genom att vända skärmen eller använda skärmskydd.
- Inte lämna informationstillgångar så som mobiltelefoner, fysiska papper eller bärbar dator oövervakade på oskyddade platser.

För medarbetare som arbetar på distans med mycket konfidentiella uppgifter eller har höga behörigheter kan ytterligare tekniska säkerhetsåtgärder, så som s-VLAN dosa, behövas. Dialog behöver föras mellan medarbetare och chef.

3.5 Medvetenhet och utbildning om informationssäkerhet och dataskydd

En god informationssäkerhet förutsätter att medarbetare är medvetna och har kunskap om hur deras beteende påverkar informationssäkerheten. Samtliga medarbetare behöver förstå

syftet och sin egen roll när det kommer till informationssäkerhet och dataskydd.

Informationssäkerhetschef ansvarar för att utbildningar inom informationssäkerhet och dataskydd finns tillgängliga.

HR-direktör ansvarar för att skapa förutsättningar för att medarbetare är medvetna, exempelvis genom att introduktionsprogram för nya medarbetare innehåller avsnitt om informationssäkerhet och dataskydd, samt att grundläggande utbildningar inom informationssäkerhet och dataskydd är obligatoriska för alla medarbetare.

Chef ansvarar för att säkerställa att medarbetare får möjlighet att utföra nödvändig utbildning inom informationssäkerhet och dataskydd.

Medarbetare ska genomföra de utbildningar kring informationssäkerhet och dataskydd som denne har identifierats ha behov av.

3.6 IT-utrustning

IT-utrustning som tillhandahålls av VGR är arbetsredskap och endast avsedda för arbetsrelaterade uppgifter.

Informationsägaren ansvarar för att förmedla säkerhetskrav på IT-utrustning till ägare av IS/IT-tjänst. Ägare av IS/IT-tjänst ansvarar för att tillhandahålla IT-utrustning och vägleda i vilken utrustning som passar för vilket ändamål.

Chef ansvarar för att dennes medarbetare har ändamålsenlig utrustning. Chef ansvarar även för att säkerställa att utrustning har återlämnats vid avslutande av tjänst eller förändrad anställning som innebär att samtliga eller delar av utrustningen behöver återkallas.

Medarbetaren är ansvarig för sin hantering av utrustning och ansvarar för att ingen obehörig får åtkomst till utrustningen. Medarbetaren ska alltid följa tillverkarens instruktioner för skydd av utrustningen, tex skydd mot vatten, värme, fukt, damm och

exponering för starka elektromagnetiska fält. Medarbetare får inte medvetet förbigå säkerhetsåtgärder, exempelvis avaktivera uppdateringar eller säkerhetsprogramvara.

Medarbetare ska lämna tillbaka utrustning till arbetsgivaren vid anställningens upphörande eller då den inte längre behövs. När utrustningen ska återlämnas eller repareras får den endast lämnas till chef eller behörig medarbetare som administrerar IT-utrustning inom VGR.

Privat IT-utrustning ska inte anslutas till regionens IT-utrustning.

3.7 Övervakning

VGR övervakar kontinuerligt IT-miljön, IS/IT-tjänster och IT-utrustning för att tidigt identifiera hot och sårbarheter, samt för att skydda verksamheten mot cyberattacker.

Det är inte tillåtet att använda anonymiseringstjänster som hindrar eller försvårar övervakning och spårning på individnivå i regionens nätverk eller informationsbehandlingsresurser, exempelvis TOR-nätverk eller privata VPN-tjänster.

Informationssäkerhetschef har mandat att blockera åtkomst via regionens nätverk till webbsidor, IS/IT tjänster och IT-utrustning som kan utsätta regionen för säkerhetsrisker.

Som arbetsgivare har VGR även rätt att vid misstanke om brott eller illojalt beteende undersöka medarbetares dator och kontrollera vilka system, webbplatser eller information som har hanterats, samt vilka filer och e-postmeddelanden som finns lagrade på enheten.

3.8 Disciplinär åtgärd

Medarbetaren kan bli föremål för disciplinära åtgärder om ledningssystemet för informationssäkerhet och dataskydd inte följs.

3.9 Vid avslut eller ändring av tjänst

När medarbetare avslutar sin tjänst ansvarar medarbetaren för att lämna tillbaka såväl information som utrustning till VGR. Medarbetare ansvarar för att omhänderta information i enlighet med informationsägarens anvisningar.

Medarbetaren förväntas dokumentera kunskap som denne besitter och som är viktig för pågående verksamhet innan anställningen avslutas eller ändras.

Relaterade dokument

- 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 (Dokument-ID: RS10162-1596316381-258)
- Konsekvensbedömning avseende dataskydd – Regional rutin 2024-2028 (Dokument-ID: RS10162-1596316381-259)
- Åtkomst till information och relaterade tillgångar – Regional rutin 2025-2029 (Dokument ID: RS 10162-1596316381-366)
- Distansarbete inom Västra Götalandsregionen – Regional rutin (Dokument-ID: RS8630-1138324516-26)
- Regiondirektörens fördelning av ansvar inom Koncernkontoret (diarienummer: RS 2023-05437)
- ISO/IEC 27002:2022 Informationssäkerhet, cybersäkerhet och integritetsskydd – Kontroller av informationssäkerhet

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Irja Burhöi, (irjbu1), Regionutvecklare

Godkänd av: Ann-Charlotte Lilja Järnström, (ancja6), Regiondirektör

Dokument-ID: RS10162-1596316381-356

Version: 2.0

Giltig från: 2025-12-28

Giltig till: 2029-12-31