Gäller för: Västra Götalandsregionen
Innehållsansvar: Jan Wallberg, (janwa18), Regionutvecklare
Granskad av: Anders Falkeby, (andfa14), Avdelningschef
Godkänd av: Johan Flarup, (johfl), Direktör

Giltig från: 2024-09-06
Giltig till: 2028-12-31

Hantering av uppgifter som är säkerhetsskydds-klassificerade, eller berör säkerhetskänslig verksamhet

Regional rutin 2024—2028

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

Sammanfattning

Inom Västra Götalandsregionen (VGR) finns det verksamheter som bedriver säkerhetskänslig verksamhet och/eller hanterar säkerhetsskyddsklassificeras uppgifter vilket kräver särskild hantering. Den här rutinen anger hur säkerhetsskyddsklassificerade uppgifter som omfattas av offentlighets- och sekretesslagen, samt hur säkerhetskänsliga uppgifter vilka omfattas av säkerhetsskyddslagen ska hanteras.

Rutinen utgår från policyn för säkerhet och beredskap och gäller för samtliga förvaltningar och bolag som bedriver säkerhetsskyddskänslig verksamhet, eller/och där säkerhetsskyddsklassificerade uppgifter eller information som berör säkerhetskänslig verksamhet förekommer eller antas förekomma. Rutinen gäller strukturerade som ostrukturerade säkerhetsskyddsklassificerade uppgifter inom VGR, oberoende om de hanteras av VGRs personal eller av extern part.

Rutinen ska användas i hanteringen av information beroende på behovet av konfidentialitet, riktighet och tillgänglighet.

När klassificering och konsekvensbedömning är klar ska hantering anpassats så att inga säkerhetsskyddsklassificerade uppgifter, samt information som berör säkerhetskänslig verksamhet, riskerar att röjas, ändras, göras otillgängliga eller förstöras av en antagonist.

Hantering av säkerhetskänsliga uppgifter

Verksamhetsutövaren är den som bedriver säkerhetskänslig verksamhet och/eller hanterar säkerhetsskyddsklassificerade uppgifter. Verksamhetsutövaren ska utreda behovet av säkerhetsskydd där en del är klassificering av säkerhetsskyddsklassificerade uppgifter och av information som berör säkerhetskänslig verksamhet.

Nedan redovisas hur säkerhetsskyddsklassificerade uppgifter ska hanteras.

Typ av hantering	Begränsat hemlig	Konfidentiell	Hemlig	Kvalificerat hemlig
Upprättande av handling	Anteckning om • Säkerhetsskyddsklass • Tillämplig sekretessbestämmelse • Datum när anteckningen gjordes • Myndighet som har gjort anteckningen • Om ursprungsland	Anteckning om • Säkerhetsskyddsklass • Tillämplig sekretessbestämmelse • Datum när anteckningen gjordes • Myndighet som har gjort anteckningen • Om ursprungsland • antal sidor och uppgift om bilagor	Anteckning om • Säkerhetsskyddsklass • Tillämplig sekretessbestämmelse • Datum när anteckningen gjordes • Myndighet som har gjort anteckningen • Om ursprungsland • antal sidor och uppgift om bilagor • exemplarnummer för fysisk handling	Anteckning om • Säkerhetsskyddsklass • Tillämplig sekretessbestämmelse • Datum när anteckningen gjordes • Myndighet som har gjort anteckningen • Om ursprungsland • antal sidor och uppgift om bilagor • exemplarnummer för fysisk handling
Utlämnande till extern	Ska sekretessprövas av informationsägare. (Vid misstanke om aggregering av utlämnad information ska ESB kontaktas)			Endast efter beslut av Regiondirektör eller honom utsedd.
Åtkomsträttighet och spårbarhet[1]	Användaren ska behöva informationen för att kunna lösa sin uppgift, är utbildad och	Användaren skall behöva informationen för att kunna lösa sin uppgift, är utbildad och	Användaren skall behöva informationen för att kunna lösa sin uppgift, är utbildad och	Användaren skall behöva informationen för att kunna lösa sin uppgift, är utbildad och

[1] Mottagande av en säkerhetsskyddad elektronisk handling behöver dock inte kvitteras om mottagandet sker i ett informationssystem där det i en säkerhets-logg noteras vem som tagit del av handlingen

	säkerhetsprövad motsvarande den nivå informationshanteringen kräver. Medveten om tystnadsplikten och gällande lagstiftning.	säkerhetsprövad motsvarande den nivå informationshanteringen kräver. Medveten om tystnadsplikten och gällande lagstiftning. Delgiven information ska kvitteras av mottagare i särskilt register al. kvitto. Kvittering skall sparas i minst 10 år.	säkerhetsprövad motsvarande den nivå informationshanteringen kräver. Medveten om tystnadsplikten och gällande lagstiftning. Delgiven information ska kvitteras av mottagare i särskilt register al. kvitto. Kvittering skall sparas i minst 10 år. Vid muntlig delgivning bör antecknas vem som tagit del.	säkerhetsprövad motsvarande den nivå informationshanteringen kräver. Medveten om tystnadsplikten och gällande lagstiftning. Delgiven information skall kvitteras av mottagare i särskilt register al. kvitto i två ex. Kvittering skall sparas i minst 25 år. Vid muntlig delgivning ska det antecknas vem som tagit del.
Behörighets-styrning	Användarstyrd åtkomstkontroll till individ/användarkonto	Användarstyrd åtkomstkontroll till individ/användarkonto	Användarstyrd åtkomstkontroll till individ/användarkonto	Användarstyrd åtkomstkontroll till individ/användarkonto (Säkerhetsskyddschef tilldelar behörighet)
Användare av digital information	Enbart på fristående dator med för **Begränsat Hemlig** information. Ska hanteras så att endast behörig personal kan ta del. Utrymme fritt från insyn	Enbart på fristående dator med Förvarsmaktskrypto för **Konfidentiell** information. Ska hanteras så att endast behörig personal kan ta del. Utrymme fritt från insyn RÖS-skyddat	Enbart på fristående dator med Förvarsmaktskrypto för **Hemlig** information. Ska hanteras så att endast behörig personal kan ta del. Utrymme fritt från insyn och [2]RÖS-skyddat	Enbart på fristående dator med Förvarsmaktskrypto för **Kvalificerat Hemlig** information. Ska hanteras så att endast behörig personal kan ta del. Utrymme fritt från insyn och RÖS-skyddat

[2] RÖS = röjande signaler (se MSB ”Riskreducerande åtgärder för lokal avsedd för delgivning av hemliga uppgifter” kap.5)

[3]Distribution av fysiska handlingar	Distribueras av egen personal alternativt leverantör. Säkerhetsförslutet engångsemballage skall användas.	Distribueras av egen personal alternativt särskilt upphandlad leverantör. Säkerhetsförslutet engångsemballage skall användas.	Distribueras av egen personal alternativt särskilt upphandlad leverantör. Säkerhetsförslutet engångsemballage skall användas.	Med bud vilket ska godkänns av Säkerhetsskyddschefen.
Hantering av uppgifter och dokument inom VGR:s lokaler	Ska hanteras så att endast behörig personal kan ta del. Fritt från insyn.	Ska hanteras så att endast behörig personal kan ta del. Fritt från insyn.	Ska hanteras så att endast behörig personal kan ta del. Fritt från insyn.	Ska hanteras så att endast behörig personal kan ta del. Fritt från insyn.
Fysiska möten	Skydd mot avlyssning samt insynsskyddat	Avlyssnings samt insynsskyddat i s.k. [4]ASK-utrymme. RÖS-skydd om elektronik används.	Avlyssnings- samt insynsskyddat i s.k. ASK-utrymme. Teknisk säkerhetsskydds-undersökning – (TSU) ska vara genomförd. RÖS-skydd om elektronik används.	Avlyssnings samt insynsskyddat i s.k. ASK-utrymme. Teknisk säkerhetsskydds-undersökning – (TSU) ska vara genomförd. RÖS-skydd om elektronik används.
Hantering av uppgifter och handling utanför VGR:s lokaler	Ska hållas under ständig uppsikt eller förvaring vilket motsvarar skyddet inom VGR lokaler.	Ska hållas under ständig uppsikt eller förvaring vilket motsvarar skyddet inom VGR lokaler.	Ska hållas under ständig uppsikt eller förvaring vilket motsvarar skyddet inom VGR lokaler.	Endast efter beslut av Säkerhetsskyddschefen eller honom utsedd.
Hantering av digital lagringsmedia	Ska vara godkänt av Signalskyddsorganisationen VGR och får endast hanteras i ett	Ska vara godkänt av Signalskyddsorganisationen VGR och får endast hanteras i ett	Ska vara godkänt av Signalskyddsorganisationen VGR och får endast hanteras i ett	Ska vara godkänt av Signalskyddsorganisationen VGR och får endast hanteras i ett

[3] Säkerhetsskyddsklassificerad information ska postas rekommenderat i säkerhetskuvert i alla led. Varje rekommenderat säkerhetskuvert har ett unikt ID-nummer. När ett rekommenderat säkerhetskuvert tas emot ska mottagare kontakta avsändaren och kontrollera ID-numret och att kuvertet kommit fram obrutet.

[4] ASK-utrymme = Avslyssningsskyddade utrymme (se SÄPO ”Vägledning i säkerhetsskydd”)

inom VGR:s lokaler	ackrediterat IT-system som motsvarar Begränsat hemlig.	ackrediterat IT-system som motsvarar Konfidentiell.	ackrediterat IT-system som motsvarar Hemlig.	ackrediterat IT-system som motsvarar Kvalificerat Hemlig.
Hantering av digital lagringsmedia utanför VGR:s lokaler	Ska hållas under ständig uppsikt med hantering och förvaring vilket motsvarar skyddet inom VGR lokaler.	Ska hållas under ständig uppsikt med hantering och förvaring vilket motsvarar skyddet inom VGR lokaler.	Ska hållas under ständig uppsikt med hantering och förvaring vilket motsvarar skyddet inom VGR lokaler.	Endast efter beslut av Säkerhetsskyddschefen eller honom utsedd. Ska hållas under ständig uppsikt med hantering och förvaring vilket motsvarar skyddet inom VGR lokaler.
Molntjänster	Endast av Försvarsmakten godkänd krypterad datakommunikation (SG R) och lagring	Endast av Försvarsmakten godkänd krypterad datakommunikation (SG S) och lagring	Endast av Försvarsmakten godkänd krypterad datakommunikation (SG S) och lagring	Endast av Försvarsmakten godkänd krypterad datakommunikation (SG TS) och lagring
[5]**Kommunikation i IT-system**	Endast av Försvarsmakten godkänd krypterad datakommunikation (SG R)	Endast av Försvarsmakten godkänd krypterad datakommunikation (SG S)	Endast av Försvarsmakten godkänd krypterad datakommunikation (SG S)	Endast av Försvarsmakten godkänd krypterad datakommunikation (SG TS)
Märkning av lagringsmedium	Säkerhetsskyddsklass och id-uppgift	Säkerhetsskyddsklass och id-uppgift	Säkerhetsskyddsklass och id-uppgift	Säkerhetsskyddsklass och id-uppgift
Medförande utanför Sveriges gränser	Efter beslut av Säkerhetsskyddschef. Ska hållas under ständig uppsikt med hantering och förvaring vilket motsvarar skyddet inom VGR lokaler.	Efter beslut av Säkerhetsskyddschef. Ska hållas under ständig uppsikt med hantering och förvaring vilket motsvarar skyddet inom VGR lokaler.	Efter beslut av Säkerhetsskyddschef. Ska hållas under ständig uppsikt med hantering och förvaring vilket motsvarar skyddet inom VGR lokaler.	Endast efter beslut av Säkerhetsskyddschefen eller honom utsedd. Ska hållas under ständig uppsikt med hantering och förvaring vilket

[5] SG R/ SG C/ SG S/ SG TS = av Försvarsmakten godkänt krypto (kontakta VGR Signalskyddsorganisation för vägledning)

				motsvarar skyddet inom VGR lokaler.
Lagring/ Förvaring	Inlåst i säkerhetsskåp (enligt SS 3492), värdeskåp (enligt SS-EN 1143–1), säkerhetsarkiv etc. i av VGR tilldelat larmat utrymme/lokal. *Gäller ej om handlingen skyddas av försvarsmaktskrypto.*	Inlåst i säkerhetsskåp (enligt SS 3492), värdeskåp (enligt SS-EN 1143–1), säkerhetsarkiv etc. i av VGR tilldelat larmat utrymme/lokal. *Gäller ej om handlingen skyddas av försvarsmaktskrypto.*	Inlåst i säkerhetsskåp (enligt SS 3492), värdeskåp (enligt SS-EN 1143–1), säkerhetsarkiv etc. i av VGR tilldelat larmat utrymme/lokal. *Gäller ej om handlingen skyddas av försvarsmaktskrypto.*	Förvaras hos Säkerhetsskyddschefen, eller av honom beslutad. Inlåst i förvaringsutrymme enligt FFS 2019:2 Skyddsnivå 4, där endast informationsägaren har tillgång, i av VGR tilldelat utrymme/lokal. *Gäller ej om handlingen skyddas av försvarsmaktskrypto.*
Utskrift	Under uppsikt, på en skrivare utan möjlighet till uppkoppling till inter/intranät och utan minnesfunktion.	Under uppsikt, på en skrivare utan möjlighet till uppkoppling till inter/intranät och utan minnesfunktion.	Under uppsikt, på en skrivare utan möjlighet till uppkoppling till inter/intranät och utan minnesfunktion.	Under uppsikt, på en skrivare utan möjlighet till uppkoppling till inter/intranät och utan minnesfunktion.
Kopiering	Under uppsikt, på kopiator utan möjlighet till uppkoppling till inter/intranät och utan minnesfunktion.	Medgivande av informationsägare med kopieringsbeslut vilket bifogas originaldokumentet. Kopia ska numreras. Under uppsikt, på kopiator utan möjlighet till uppkoppling till inter/intranät och utan minnesfunktion	Medgivande av informationsägare med kopieringsbeslut vilket bifogas originaldokumentet. Kopia ska numreras. Under uppsikt, på kopiator utan möjlighet till uppkoppling till inter/intranät och utan minnesfunktion	Endast efter beslut av Säkerhetsskyddschef eller honom utsedd. Medgivande av informationsägare med kopieringsbeslut vilket bifogas originaldokumentet. Kopia ska numreras
Kopia eller utdrag	Den som tar del ska upplysas om innebörden av sekretessen.	Medgivande av informationsägare med utdragsbeslut vilket bifogas originaldokumentet. Utdrag ska numreras. Den som tar del ska	Medgivande av informationsägare med utdragsbeslut vilket bifogas originaldokumentet. Utdrag ska numreras. Den som tar del ska	Endast efter beslut av Säkerhetsskyddschef. Medgivande av informationsägare med utdragsbeslut vilket bifogas originaldokumentet. Utdrag ska

		upplysas om innebörden av sekretessen.	upplysas om innebörden av sekretessen.	numreras. Den som tar del ska upplysas om innebörden av sekretessen.
Förstöring av dokument/ utrustning	Med [6]dokumentförstörare där restprodukterna får utgöras av spån med en bredd av högst 2,5 mm och en längd av högst 30 mm eller av högst 4 x 4 mm kvadratiska spån, alternativt kontrollerad bränning. För förstöring av lagringsmedier kontakta ASB.	Med dokumentförstörare där restprodukterna får utgöras av spån med en bredd av högst 1,2 mm och en längd av högst 15 mm eller av högst 2 x 2 mm kvadratiska spån, alternativt kontrollerad bränning. Ska dokumenteras För förstöring av lagringsmedier kontakta ASB.	Med dokumentförstörare där restprodukterna får utgöras av spån med en bredd av högst 1,2 mm och en längd av högst 15 mm eller av högst 2 x 2 mm kvadratiska spån, alternativt kontrollerad bränning. Två personer närvarande Ska dokumenteras För förstöring av lagringsmedier kontakta ASB.	Med dokumentförstörare där restprodukterna får utgöras av spån med en bredd av högst 1,2 mm och en längd av högst 15 mm eller av högst 2 x 2 mm kvadratiska spån, alternativt kontrollerad bränning. Två personer närvarande. Ska dokumenteras För förstöring av lagringsmedier kontakta ASB.
Videokonferens	Endast av Försvarsmakten och VGR godkänt signalskyddssystem för Begränsat Hemlig	Endast av Försvarsmakten och VGR godkänt signalskyddssystem för Konfidentiell	Endast av Försvarsmakten och VGR godkänt signalskyddssystem för Hemlig	Endast av Försvarsmakten och VGR godkänt signalskyddssystem för Kvalificerat Hemlig
Mobiltelefon, motsv.	Endast med krypterat tal (SG R) Förvarsmaktskrypto.	Endast med krypterat tal (SG S) Förvarsmaktskrypto.	Endast med krypterat tal (SG S) Förvarsmaktskrypto.	Finns ej
Mejl, fax etc.	Försvarsmaktskrypto godkänt för Begränsat Hemlig (SG R)	Försvarsmaktskrypto godkänt för konfidentiell (SG S)	Försvarsmaktskrypto godkänt för hemlig (SG S)	Försvarsmaktskrypto godkänt för kvalificerat hemlig (SG TS)

[6] Får inte användas för förstöring av handling som är placerade högre än ”Begränsat hemlig”. Ska märkas med *”Endast för förstöring av Begränsat Hemlig”*

[7]Inkommen handling	Sekretessprövas	Sekretessprövas	Sekretessprövas	Sekretessprövas
[8]Överföring av sekretess	Kontroll ska genomföras om det finns en bestämmelse att sekretessen gäller uppgiften efter överföring. Det kan vara mellan myndigheter och verksamheter inom myndigheten, vilka är att betrakta som självständiga i förhållande till varandra.	Kontroll ska genomföras om det finns en bestämmelse att sekretessen gäller uppgiften efter överföring. Det kan vara mellan myndigheter och verksamheter inom myndigheten, vilka är att betrakta som självständiga i förhållande till varandra	Kontroll ska genomföras om det finns en bestämmelse att sekretessen gäller uppgiften efter överföring. Det kan vara mellan myndigheter och verksamheter inom myndigheten, vilka är att betrakta som självständiga i förhållande till varandra	Kontroll ska genomföras om det finns en bestämmelse att sekretessen gäller uppgiften efter överföring. Det kan vara mellan myndigheter och verksamheter inom myndigheten, vilka är att betrakta som självständiga i förhållande till varandra.
[9]Arkivering, registrering, diarieföring etc.	Om en sekretessreglerad uppgift överförs från annan myndighet blir sekretessbestämmelsen tillämplig även här. I övrigt se Informationssäkerhet och dataskydd - Koncernkontoret (vgregion.se)	Om en sekretessreglerad uppgift överförs från annan myndighet blir sekretessbestämmelsen tillämplig även här. I övrigt se Informationssäkerhet och dataskydd - Koncernkontoret (vgregion.se)	Om en sekretessreglerad uppgift överförs från annan myndighet blir sekretessbestämmelsen tillämplig även här. I övrigt se Informationssäkerhet och dataskydd - Koncernkontoret (vgregion.se)	Om en sekretessreglerad uppgift överförs från annan myndighet blir sekretessbestämmelsen tillämplig även här. I övrigt se Informationssäkerhet och dataskydd - Koncernkontoret (vgregion.se)

[7] Vid tvekan se SFS 2009:400, alt. samverka med ESB eller Juridik.
[8] Vid tvekan se SFS 2009:400, alt. samverka med ESB eller Juridik.
[9] Se även OSL SFS 2009:400 11 kap. 6 §

Definitioner

Säkerhetsskyddsklassificerade uppgifter

Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.

Säkerhetskänslig verksamhet

Säkerhetskänslig verksamhet är sådan verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.

Samhällsviktig verksamhet

Verksamheter som rör leveranser, tjänster och funktioner som är nödvändiga för samhällets funktionalitet på nationell nivå.

Konfidentialitet

Att förhindra att information röjs för obehöriga.

Sekretess

Inskränkning i offentlighetsprincipen. Förbud att röja en uppgift, muntligen eller lämna ut handling.

Offentlighets- och sekretesslagen

Bestämmelser som beskriver om när en uppgift omfattas av sekretess.

Riktighet

Egenskap hos informationstillgång som innebär att den skyddas mot oönskad förändring.

Tillgänglighet

Informationen är tillgänglig när den behövs.

Spårbarhet

Entydig härledning av utförda aktiviteter till en identifierad användare.

Tillgänglighet

Egenskap hos informationstillgång som innebär att den är åtkomlig och användbar inom förväntad tid och omfattning.

Strukturerad information

Information som görs sökbar genom att den följer givna regler där metadata informerar om, och gör informationen tillgänglig.

Ostrukturerad information

Informationen är inte kopplad eller enkelt sökbar i något system utan behöver tolkas.

Relaterade dokument

Inom området säkerhetsskydd finns det ett antal olika styrdokument. Regionövergripande styrdokument finns på intranätet under Styrande dokument - säkerhet och beredskap - VGR gemensamt (vgregion.se)

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Jan Wallberg, (janwa18), Regionutvecklare

Granskad av: Anders Falkeby, (andfa14), Avdelningschef

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-151

Version: 4.0

Giltig från: 2024-09-06

Giltig till: 2028-12-31