

# Säkerhetskyddsplan för Västra Götalandsregionen

Reviderad september 2010, beslut i regionstyrelsen 28 september 2010

## Förord

### Säkerhetsskydd

Ansvar vad gäller säkerhetsskydd regleras bland annat i Säkerhetsskyddslagen (1996:627), Säkerhetsskyddsförordningen (1996:633), Rikspolisstyrelsens föreskrifter och allmänna råd om säkerhetsskydd (RPSFS 2010:03, FAP 244-1) och offentlighets- och sekretesslagen (2009:400).

Innehållet i dessa författningar har varit styrande vid framtagandet av denna plan.

Med säkerhetsskydd avses

1. Skydd mot brott som kan hota rikets säkerhet.
2. Skydd av hemliga uppgifter som rör rikets säkerhet
3. Skydd mot terrorism

Inom Västra Götalandsregionen är det Prehospitalt och Katastrofmedicinskt Centrum/ PKMC som har det övergripande och samordnande ansvaret för katastrofberedskap och säkerhetsskydd.

Säkerhetsskyddsplanen för Västra Götalandsregionen syftar till:

- att klarlägga regler för regionens säkerhetsskydd.
- att vara vägledning för det lokala arbetet med säkerhetsskyddet.
- att vara underlag för information och utbildning gällande säkerhetsskydd som skall ges till all personal.

Planen reglerar säkerhetsskyddsarbetet i fred, i kris och inför beredskapshöjning. PKMC svarar för kontinuerlig revidering av planen.

### Säkerhetspolicy

Säkerhetsstrategiska avdelningen vid regionkansliet leder och samordnar organisationen av säkerhetsarbetet i Västra Götalandsregionen. Avdelningen har bland annat tagit fram informationssäkerhetsreglemente, en säkerhetspolicy för Västra Götalandsregionen jämte ramverk och riktlinjer för säkerhetsarbetet som bildar grunden för arbetet med att hantera säkerhetsfrågorna på regional nivå.

Göteborg 10 september 2010

VÄSTRA GÖTALANDSREGIONEN  
Prehospitalt och Katastrofmedicinskt Centrum

Annika Hedelin  
Beredskaps- och säkerhetsskyddschef

## INNEHÅLLSFÖRTECKNING

1.	SÄKERHETSSKYDD	1
2.	ANSVAR OCH ORGANISATION	1
3.	SÄKERHETS- OCH SKYDDSÅTGÄRDER	2
4.	INFORMATIONSSÄKERHET	2
4.1	Handlingar och dokument	3
4.2	IT-säkerhet	4
4.3	Kommunikations- och sambandsutrustning	5
5.	FYSISK SÄKERHET	5
6.	ADMINISTRATIV SÄKERHET OCH ÅTGÄRDER VID UPPTÄCKTA OEGENTLIGHETER ELLER MISSBRUK	6
6.1	Administrativ säkerhet	6
6.2	Åtgärder vid upptäckta oegentligheter eller missbruk	6
7.	BEREDSKAP OCH PLANER	7
7.1	Katastrof och beredskap	7
7.2	Säkerhetsprövning	7
7.3	Säkerhetsklass	8
8.	SKYDDAD UPPHANDLING (SUA)	8
9.	SÄRSKILDA FÖRESKRIFTER	8
10.	BEGREPP	9
11.	KÄLLFÖRTECKNING	10

## 1. SÄKERHETSSKYDD

Sjukvårdshuvudmannen är enligt säkerhetsskyddslagen (1996:27) och säkerhetsskyddsförordningen (1996:633) skyldig att ha ett fungerande säkerhetsskydd som skall säkerställa att

- säkerhetskänslig information som avser rikets säkerhet inte röjs, ändras eller förstörs (informationssäkerhet)
- obehöriga hindras från att få tillträde till platser där de kan få tillgång till sådan information, eller där verksamhet bedrivs, som har betydelse för rikets säkerhet (tillträdesskydd)
- personer som inte är pålitliga ur säkerhetssynpunkt ej deltar i ovannämnda verksamhet.

Regionens ansvar omfattar också olika typer av skydd och åtgärder för att trygga omfattande och viktiga verksamheter. Exempel på sådana åtgärder är skydd av patienter och personal, produktion och driftverksamhet, brandskydd, tillträdesskydd, informations- och IT-säkerhet, medicinsk och teknisk säkerhet, arbetsmiljö, katastrof-, beredskaps- och säkerhetsplanläggning.

Västra Götalandsregionen bedöms inte ha anläggningar eller verksamheter som skall skyddas enligt säkerhetsförordningen (1996:633) 5§, med undantag av vissa totalförsvarsuppgifter för regionledningen under höjd beredskap.

Regionen upprätthåller en allmän säkerhetsnivå som styrs av andra lagar, förordningar, allmänna råd, policies och riktlinjer.

## 2. ANSVAR OCH ORGANISATION

Ansvaret för regionens totala verksamheter och säkerhetsskydd vilar på regionstyrelsen och regiondirektören. I säkerhetsskyddsarbetet biträds dessa av regionens säkerhetsskyddschef.

Förvaltnings- och verksamhetschefer i linjeorganisationen har ansvar för säkerhetsskyddet inom det egna verksamhetsområdet.

För att motverka brott och för att trygga och bibehålla förtroendet för regionens verksamheter måste skydd och säkerhet skapas genom

- att följa de lagar som påverkar och ställer särskilda krav på regionens verksamheter.
- att varje medarbetares viktiga funktion i säkerhetsarbetet betonas.
- att information och utbildning om hot och risker genomföres.
- att utarbeta säkerhetsrutiner så att patient- och personalsäkerhet tryggas.
- att återkommande risk- och sårbarhetsanalyser sker.

Denna säkerhetsskyddsplan har upprättats i enlighet med bestämmelserna i säkerhetsskyddsförordningen (1996:633) 5 § samt bestämmelserna i säkerhetsskyddslagen (1996:627).

Säkerhetsskyddsplanen fastställs av regionstyrelsen.

### 3. SÄKERHETS- OCH SKYDDSÅTGÄRDER

Inriktningen på säkerhetsarbetet är att förebygga risker och skador genom kostnadseffektiva säkerhetslösningar.

Säkerhetsområdena indelas i:

- Informationssäkerhet
- Fysisk säkerhet
- Administrativ säkerhet
- Säkerhetsprövning
- Beredskap och planer
- Särskilda föreskrifter

Säkerhetskrav, säkerhetsrutiner och planer skall utformas så att man vid en situation då beredskapsrutiner måste tillgripas i största möjliga mån kan bibehålla ordinarie ledningsstruktur och ordinarie arbetssätt och rutiner.

Inom Västra Götalandsregionen har säkerhetsstrategiska avdelningen ansvaret för framtagandet av säkerhetspolicy och reglemente för informationssäkerhet. Reglementet antogs vid beslut i regionfullmäktige 2000. Säkerhetspolicy för Västra Götalandsregionen antogs av regionfullmäktige 2002 och är senast uppdaterad 2008-02-11. Dessutom finns framtaget regional strategi för säkerhetsarbetet i Västra Götalandsregionen 2008-2011 (beslut RS 2008-03-04, RF 2008-04-22) och riktlinjer för informationssäkerhet i Västra Götalandsregionens verksamheter (beslut RS 2009-06-23).

### 4. INFORMATIONSSÄKERHET

Utvecklingen på informationsområdet har medfört att skyddet av sekretessbelagd information har fått en ny innebörd. Därför används termen informationssäkerhet i stället för, som tidigare, sekretesskydd.

Informationssäkerheten syftar till att hindra obehöriga att få kännedom om sekretessbelagda uppgifter som har betydelse för totalförsvaret eller för rikets säkerhet i övrigt. Dessutom ska informationssäkerheten hindra att sekretessbelagda uppgifter ändras eller förstörs.

För att få ta del av säkerhetskänsliga uppgifter måste en person

- bedömas som pålitlig ur säkerhetssynpunkt,
- ha tillräckliga kunskaper om säkerhetsskydd,
- behöva uppgifter för sitt arbete i den verksamhet där de hemliga uppgifterna förekommer.

Den som ges behörighet skall upplysas om vad sekretessen innebär. Det bör särskilt påpekas att det mest centrala kriteriet vid avgörandet om en personal skall få ta del av hemliga uppgifter är, att hon/han måste få ta del av dem för att kunna lösa sina arbetsuppgifter. Oavsett vilken ställning personen för övrigt har, gäller detta. Det spelar heller ingen som helst roll om personen aldrig så väl uppfyller de övriga två kriterierna.

Informationssäkerheten omfattar:

- Handlingar och dokument
- Data/IT-media (inkl den utrustning sådana media hanteras i)
- Sambands- och kommunikationsrutiner
- Sammanställningar av information från olika källor och som kan ge helhetsbilder/helhetssammanhang av säkerhetskänslig natur (t ex riskanalyser, sårbarhetsanalyser, riskanalysskator, kartor med olika slags information sammanförda med hjälp av geografisk informationssystemteknik m m). Varje delinformation för sig kan vara hur öppen som helst, men sammanställda med annan likartad delinformation kan man oavsiktligt och omedvetet skapa en helhetsinformation som blir säkerhetskänslig.

## 4.1 Handlingar och dokument

Hantering av hemliga handlingar regleras i säkerhetsskyddsförordningens 9-13 paragrafer.

Handling som innehåller information som omfattas av säkerhetsskyddslagen ska tydligt märkas, "hemligstämplas". Av märkningen skall framgå

- tillämplig bestämmelse i sekretesslagen
- datum för anteckningen
- vilken myndighet/enhet som klassificerat handlingen

Om en handling försvunnit eller om det kan misstänkas att informationen, som omfattas av säkerhetsskydd, röjts skall detta omedelbart anmälas till säkerhetsskyddschefen.

Administrativ säkerhet ska garantera att god säkerhet tryggas vid handläggning och rutiner beträffande:

- Registrering och handhavande av hemliga handlingar och dokument
- Förvaring och försändning av handlingar
- Sekretessregler och sekretesskydd

Handlingar inom ramen för regionens totalförsvarsuppgifter registreras i det öppna diariet vid regionstyrelsens kansli.

Registrering och arkivering av hemliga handlingar utförs av regionens säkerhetsskyddschef enligt gällande bestämmelser.

Cheferna för regionens sjukhusområden samt i förekommande fall beredskapssamordnare vid övriga förvaltningar och verksamheter skall på motsvarande sätt vid behov förvara hemliga handlingar enligt gällande bestämmelser. Förvaring, handhavande och försändning av hemliga uppgifter kräver särskilt skydd och tillämpningen regleras genom föreskrifter i säkerhetsskyddslagen och säkerhetsskyddsförordningen.

## 4.2 IT-säkerhet

IT-säkerheten är en viktig del av informationssäkerheten. Den snabba utvecklingen har medfört att användningen av datorer och telekommunikation ökat kraftigt och - som en följd härav - också metoder för obehöriga att komma åt uppgifter.

Det är den myndighet som beslutar att anskaffa eller förändra ett IT-system som skall svara för att säkerhetsskyddet tillgodoses i och kring systemet. Myndigheten är skyldig att dels göra en sekretessbedömning av såväl de enskilda uppgifter som den totala informationsmängden i systemet, dels genomföra och dokumentera risk- och sårbarhetsanalyser. Det åligger också myndigheten att se till att säkerhetsskyddet upprätthålls även under utveckling, drift och förvaltning av systemet och att skyddet mot obehörig avlyssning av röjande signaler (RÖS-skydd) är betryggande.

Nätverken kan i säkerhetsskyddshänseende utgöra en risk. Den allt snabbare utvecklingen av analysprogram för att automatiskt hitta svagheter i datorer och nätverk, gör att många fler personer än tidigare kan lyckas göra intrång i IT-systemen. Datakompetensen behöver heller inte vara särskilt hög hos de personer som gör intrångsförsök.

Det finns risker med att ladda ner dataprogram från externa källor, t ex Internet och olika databaser. Vissa av dessa program kan innehålla s k bakdörrar, vilket innebär att man t ex från Internet kan göra intrång i det nätverk som programmet laddats ned till. Program som laddas ner från externa källor kan även innehålla datavirus.

Observera att s k USB-minnen snabbt kan ”tanka ur” information från en påslagen dator. För att skydda känslig information är det viktigt att USB-minnena är lösenordsskyddade.

Vidare bör observeras att kopiering av handlingar som sker på multikopiatorer innebär att kopiatorn är försedd med en hårddisk där all information som kopieras mellanlagras. Det är därför lämpligt att antingen avtala om hur det skall förfaras med hårddisken (ett råd är att den stannar kvar och förstörs genom myndighetens försorg). Ett annat alternativ är att hårddisken plomberas av den myndighet som har full kontroll över den.

Hotbilden mot en organisations IT-verksamhet varierar kraftigt beroende på organisationens verksamhet. En analys av aktuell verksamhet ger svar på de specifika hot som är aktuella. I stora drag är det tre risker som är aktuella i någon form:

- Informationen förstörs
- Informationen stjäls
- Informationen ändras

Vad som är känsligt i en organisation är givetvis inte liktydigt med att det är känsligt i en annan. Inom sjukvården är sekretess av avgörande betydelse. Forskningsresultat och/eller patientuppgifter är exempel på information som kan utnyttjas i både gott och ont syfte.

Säkerhetsnivån för verksamhetens information skall fastställas genom att riskanalyser genomförs. Beslut om åtgärder som fattas utifrån riskanalysen skall vara väl förankrade hos ledning och personal.

IT-säkerhetsarbetet skall vara en naturligt integrerad del av en organisations verksamhet. Det skall finnas en IT-säkerhetspolicy som väl följer organisationens verksamhetsplan och som är förankrad hos ledningen. IT-direktören verkställer och ansvarar för Västra Götalandsregionens IT-strategi, tillhörande regelverk och den övergripande i IT-strukturen i Västra Götalandsregionen.

### 4.3 Kommunikations- och sambandsutrustning

Västra Götalandsregionen disponerar kryptofax och kryptotelefon för att kunna kommunicera totalförsvarsuppgifter mellan olika myndigheter. Här gäller särskilda bestämmelser som framgår i ”Handbok Totalförsvarets Signalskyddstjänst” (H TST Grunder 2007) och särskilt skydd enligt säkerhetsskyddsförordningens 13 paragraf.

## 5. FYSISK SÄKERHET

Fysisk säkerhet omfattar både byggnadsteknisk säkerhet och personsäkerhet.

*Exempel på säkerhetskrav inom det byggnadstekniska området är:*

- Egendomsskydd, t ex byggnadskonstruktioner, sektioneringar, lås och stängsel
- Inbrottslarm
- Brandlarm och brandutrustning
- Märkning/stöldskydd
- Planer för utrymning
- Reservkraft och övrigt försörjningsskydd, t ex sjukvårdens säkerhet i kris (SSIK-åtgärder)

*Exempel på personsäkerhet:*

- Patient/passagerar- och personalsäkerhet
- Yttre och inre tillträdesskydd
- Kontroll av in- och utpassering
- Anvisningar för hot- och våldssituationer samt krishantering
- Arbetsmiljöfrågor

Tillträdesbegränsningen kan utformas på olika sätt. I vissa fall räcker det med att tillträdesförbudet avser utomstående. I andra fall kan det behöva omfatta även en del av den egna personalen. För särskilt känsliga delar kan rätten till tillträde begränsas till endast de anställda som för att kunna utföra sitt arbete behöver vistas i det aktuella området. I säkerhetsskyddslagen sägs att begränsningar skall utformas så att allmänhetens rätt att röra sig fritt inte inskränks mer än nödvändigt.

Bedömning av vilka åtgärder som är lämpliga måste avgöras från fall till fall.

## 6. ADMINISTRATIV SÄKERHET OCH ÅTGÄRDER VID UPPTÄCKTA OEGENTLIGHETER ELLER MISSBRUK

### 6.1 Administrativ säkerhet

Administrativ säkerhet ska garantera att god säkerhet tryggas vid handläggning och rutiner beträffande:

- Registrering och handhavande av hemliga handlingar och dokument
- Förvaring och försändning av handlingar
- Sekretessregler och sekretesskydd

Handlingar inom ramen för regionens totalförsvarsuppgifter registreras i det öppna diariet vid regionstyrelsens kansli.

Registrering och arkivering av hemliga handlingar utförs av regionens säkerhetsskyddschef enligt gällande bestämmelser.

Cheferna för regionens sjukhusområden samt i förekommande fall beredskapssamordnare vid övriga förvaltningar och verksamheter skall på motsvarande sätt vid behov förvara hemliga handlingar enligt gällande bestämmelser. Förvaring, handhavande och försändning av hemliga uppgifter kräver särskilt skydd och tillämpningen regleras genom föreskrifter i säkerhetsskyddslagen och säkerhetsskyddsförordningen.

#### **Behörighet att ta del av hemliga uppgifter, sekretessbevis:**

Samtliga nedanstående krav skall vara uppfyllda för att vederbörande skall anses behörig:

- 1) Personen bedöms som pålitlig ur säkerhetssynpunkt. Denna bedömning grundas på den säkerhetsprövning som skall genomföras i varje enskilt fall.
- 2) Personen har tillräckliga kunskaper om säkerhetsskydd.
- 3) Personen behöver uppgifterna för sitt arbete i den verksamhet där de hemliga uppgifterna förekommer.

Den som tillåts ta del av hemliga uppgifter skall upplysas om räckvidden och innebörden av sekretessen. Denna upplysning kan ske genom att myndigheten upprättar ett s.k. sekretessbevis som undertecknas av den som upplysningen avser.

### 6.2 Åtgärder vid upptäckta oegentligheter eller missbruk

Oegentligheter är avsiktliga/medvetna fel i handläggning eller åtgärder, t ex ekonomiska oegentligheter, dataintrång, missbruk av tjänsteställning, missbruk av sekretess, mutor, jäv etc.

Förekommer misstanke om eller konstaterat fall av oegentligheter eller missbruk, skall anmälan omgående ske till närmast högre chef och till säkerhetsskyddschef.

Dessa överväger lämpligen följande åtgärder:

### **Omedelbart**

Bedöm risken för fortsatt eller utökad skada för regionen/verksamheten, för tredje man eller för den anställda.

Ta, med hänsyn till ovanstående risker, ställning till

- om den anställda skall behålla behörighet till datasystem, hantering av kontanta medel, sekretessbelagt material, nycklar etc.
- om något material behöver omhändertas för kommande utredning.
- om åtgärder behöver vidtas mot annan myndighet eller tredje man.

Syftet med den omedelbara rapporteringen är att man inom verksamheten genast ska kunna vidta åtgärder för att komma tillrätta med de fel och brister som har uppmärksamats. Fel eller brister som noteras ska omedelbart utredas och dokumenteras. Oegentligheter ska alltid rapporteras.

### **Fortsatt handläggning**

En utredning görs som kan resultera i polisanmälan. Om frågan leder till ett fortsatt personalärende avgörs i det enskilda fallet.

## **7. BEREDSKAP OCH PLANER**

### **7.1 Katastrof och beredskap**

Beredskapsplaneringen skall säkerställa att nödvändig verksamhet kan bedrivas även i ett allvarligt stort läge. Planeringen ska i första hand inriktas på rutiner för att kunna möta fredstida svåra påfrestningar på samhället och särskilda händelser inom regionen vid kriser.

En regional katastrofmedicinsk plan har fastställts av regionstyrelsen. Denna plan utgör grunden för sjukhusens och primärvårdens lokala planer.

### **7.2 Säkerhetsprövning**

Med säkerhetsprövning menas åtgärder som skall förebygga att en person som inte är pålitlig ur säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet. Prövningen skall också förebygga terrorism.

Säkerhetsprövningen består av:

- 1) den personliga kännedom som finns om den som prövningen gäller
- 2) uppgifter som framgår av betyg, intyg och referenser m m
- 3) i förekommande fall – uppgifter som framkommit vid registerkontroll och särskild personutredning.

Innan registerkontroll och särskild personutredning får göras skall den som säkerhetsprovningen gäller ha gett sitt samtycke till åtgärden. Samtycket anses gälla också förnyade kontroller och utredningar så länge som den kontrollerade innehar samma anställning. Säkerhetsprovning utförs av säkerhetspolisen (SÄPO).

### **7.3 Säkerhetsklass**

Regionen beslutar om placering i säkerhetsklass 2 och 3 för enskilda som bedriver säkerhets känslig verksamhet, medan regeringen fattar beslut om placering i säkerhetsklass 1.

För säkerhetsklasserna 1 och 2 gäller att ny registerkontroll skall göras minst vart femte år samt om befattningshavaren gift sig, inlett - eller avbrutit - ett samboförhållande efter den senaste registerkontrollen.

## **8. SKYDDAD UPPHANDLING (SUA)**

I de fall då regionen avser att begära in anbud eller träffa avtal om upphandling som med hänsyn till rikets säkerhet skall hållas hemlig, skall regionen träffa en skriftlig överenskommelse (säkerhetsskyddsavtal) med anbudsgivaren eller leverantören om vilket säkerhetsskydd som behövs i det särskilda fallet.

Allmänt gäller att regionen, innan en upphandling påbörjas, är skyldig att pröva om upphandlingen helt eller delvis skall omges av säkerhetsskydd.

Skall upphandlingen omges av ett säkerhetsskydd åligger det regionen att fortlöpande pröva och anpassa skyddet med anpassning till aktuell hotbild, upphandlingens omfattning och skyddsvärdet hos de uppgifter som kommer att hanteras av det företag hos vilken upphandlingen sker.

Regionen skall underrätta SÄPO om dels säkerhetsskyddsavtal som har träffats och dels om säkerhetsskyddsavtal som har upphört att gälla. Kontakt sker med SÄPO via säkerhetsskyddschef.

Säkerhetspolisen har gett ut en handbok för säkerhetsskyddad upphandling med säkerhetsskyddsavtal.

## **9. SÄRSKILDA FÖRESKRIFTER**

Varje förvaltning skall, med beaktande av gällande bestämmelser, ta fram föreskrifter för

- hur kvittering eller anteckning skall göras när hemlig handling delges muntligt eller genom visning
- hur återlämnande av kvitterade hemliga handlingar skall gå till
- hur tillfällig respektive varaktig förvaring av hemliga handlingar skall gå till
- hur och när hemliga handlingar skall inventeras
- hur hemliga handlingar skall tas emot och sändas inom respektive förvaltning
- hur förvaltningen reglerar tillträdesbestämmelser för platser där känslig verksamhet bedrivs
- hur förvaltningen reglerar tillträde till och ansvar för förvaringsutrymme för hemliga handlingar.

## 10. BEGREPP

### **Hemlig handling**

Handling som innehåller hemlig uppgift.

### **Hemlig uppgift**

Uppgift som omfattas av sekretess enligt sekretesslagen och som rör rikets säkerhet.

### **Informationssäkerhet**

Åtgärder som skall förebygga att hemlig uppgift obehörigen röjs, ändras eller förstörs.

### **IT-säkerhet**

Förkortning för informationsteknisk säkerhet, som är en viktig del av informationssäkerheten. IT-säkerhet kan indelas i datasäkerhet och kommunikationssäkerhet.

### **Registerkontroll**

Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller polisdata-lagen (1998:622). Med registerkontroll avses också att sådana personuppgifter hämtas som rikspolisstyrelsen eller SÄPO behandlar utan att de ingår i ett sådant register som avses i första stycket. Med registerkontroll avses dock inte att uppgifter hämtas från en förundersökning eller särskild undersökning i kriminalunderrättelseverksamhet.

### **Säkerhetsanalys**

Myndigheter, och andra som säkerhetsskyddsförordningen gäller för, skall undersöka vilka uppgifter i deras verksamhet som skall hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Resultatet av denna undersökning (säkerhetsanalys) skall dokumenteras.

### **Säkerhetsklass**

Anställning eller visst slag av deltagande skall under vissa förutsättningar placeras i säkerhetsklass. Det finns tre olika säkerhetsklasser, säkerhetsklass 1, 2 eller 3. Tillhörigheten till säkerhetsklass beror främst på mängden hemliga uppgifter som delges den anställde eller den deltagande.

### **Säkerhetsprövning**

En prövning som skall göras av en myndighet m.fl. innan en person genom anställning eller på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet eller anlitas för sysslor som är viktiga för skyddet mot terrorism. Prövningen skall förebygga dels att personer som inte är pålitliga ur säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet och dels terrorism. I vissa fall skall säkerhetsprövningen omfatta registerkontroll och särskild personutredning.

### **Säkerhetsskydd**

Åtgärder till skydd mot spioneri, sabotage och andra brott som rör rikets säkerhet, skydd i andra fall av hemliga uppgifter och skydd mot terrorism – även terrorism som inte hotar rikets säkerhet. Olika säkerhetsskyddsåtgärder är informationssäkerhet, tillträdesbegränsning och säkerhetsprövning. I säkerhetsskyddet ingår också utbildning och kontroll.

### **Säkerhetsskyddsavtal**

När staten, kommuner och regioner/landsting avser att begära in anbud eller träffa avtal om upphandling där det förekommer hemliga uppgifter, skall var och en av ovanstående myndigheter träffa ett skriftligt avtal med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det enskilda fallet.

### **Tillträdesbegränsning**

Åtgärder som skall förebygga att obehöriga får tillträde till platser där de kan få tillgång till hemliga uppgifter, eller där det bedrivs verksamhet som har betydelse för rikets säkerhet.

## **11. KÄLLFÖRTECKNING**

- Säkerhetsskyddslag, 1996:627
- Säkerhetsskyddsförordning, 1996:633
- Rikspolisstyrelsens författningssamling 2010:03 FAP 244-1
- Säkerhetsskydd – en vägledning, Säkerhetspolisen, senast reviderad januari 2010
- Författningshandbok för totalförsvaret och skydd mot olyckor 2009/2010

The background is a solid yellow color with several large, overlapping, curved shapes in a slightly darker shade of yellow, creating a sense of depth and movement. The shapes are organic and fluid, resembling stylized waves or abstract architectural forms.

Västra Götalandsregionen  
Prehospitalt och Katastrofmedicinskt Centrum  
405 44 GÖTEBORG  
[www.vgregion.se/pkmc](http://www.vgregion.se/pkmc)

September 2010