Polismyndighetens författningssamling

ISSN 2002-0139
Utgivare: Gunilla Hedwall

Säkerhetspolisens föreskrifter om säkerhetsskydd;

PMFS 2022:1

beslutade den 31 januari 2022.

Utkom från trycket
den 4 februari 2022

Säkerhetspolisen föreskriver följande med stöd av 3 kap. 10 § och 8 kap. 6 § säkerhetsskyddsförordningen (2021:955).

1 kap. Allmänna bestämmelser

Föreskrifternas innehåll

1 § Dessa föreskrifter innehåller kompletterande bestämmelser till säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2021:955).

Innehållet i föreskrifterna är uppdelat enligt följande:

1 kap. – Allmänna bestämmelser
2 kap. – Grundläggande bestämmelser om säkerhetsskydd
3 kap. – Informationssäkerhet
4 kap. – Informationssäkerhet i och kring informationssystem
5 kap. – Fysisk säkerhet
6 kap. – Personalsäkerhet
7 kap. – Skyldigheter när en annan aktör kan få tillgång till säkerhetskänslig verksamhet
8 kap. – Överklagande och undantag från föreskrifterna

Föreskrifternas tillämpning på försvarsområdet

2 § För Försvarsmakten och Försvarets materielverk samt verksamhetsutövare inom deras tillsynsområden gäller endast bestämmelserna om förfarandet vid registerkontroll i 6 kap. 7–15 §§.

Företräde för bestämmelser i vissa internationella överenskommelser

3 § Om det i en överenskommelse som avses i 10 kap. 1 eller 2 § regeringsformen som rör ett visst internationellt samarbete förekommer bestämmelser om säkerhetsskydd som avviker från dessa föreskrifter, ska bestämmelserna i överenskommelsen ha företräde, under förutsättning att de inte strider mot en bestämmelse i lag eller förordning.

Krav på dokumentation

4 § Bedömningar, beslut, planer och åtgärder samt uppföljning enligt föreskrifterna ska dokumenteras.

5 § I dessa föreskrifter avses med

1. *dimensionerande antagonistiska förmågor*: antagonistiska förmågor som vissa säkerhetsskyddsåtgärder ska dimensioneras utifrån, oavsett om de motsvaras av något identifierat säkerhetshot mot den säkerhetskänsliga verksamheten eller inte,
2. *intrångsdetektering*: administrativa eller tekniska åtgärder som vidtas för att detektera intrång eller försök till intrång i informationssystem,
3. *intrångsskydd*: administrativa eller tekniska åtgärder som vidtas för att skydda informationssystem mot obehörig åtkomst,
4. *röjande signaler*: elektromagnetiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs,
5. *skadlig kod*: oönskad programkod som är till för att ändra, röja, förstöra eller avlyssna elektronisk kommunikation eller funktioner eller uppgifter i ett informationssystem, och
6. *tillsynsmyndighet*: myndighet som utövar tillsyn enligt 8 kap. 1 § säkerhetsskyddsförordningen (2021:955).

Ord och uttryck i föreskrifterna har i övrigt samma innebörd som i säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen.

2 kap. Grundläggande bestämmelser om säkerhetsskydd

Säkerhetsskyddsanalys

Innehåll

1 § Av 2 kap. 1 § säkerhetsskyddslagen (2018:585) och 2 kap. 1 § säkerhetsskyddsförordningen (2021:955) följer att den som till någon del bedriver säkerhetskänslig verksamhet ska göra en säkerhetsskyddsanalys.

En säkerhetsskyddsanalys ska innehålla de moment som framgår av 2–9 §§.

Verksamhetsbeskrivning

2 § Verksamhetsutövaren ska övergripande beskriva sin verksamhet och specificera vilka delar av verksamheten som är av betydelse för Sveriges säkerhet utifrån kategorierna Sveriges yttre säkerhet, Sveriges inre säkerhet, nationellt samhällsviktig verksamhet, verksamhet av betydelse för Sveriges ekonomi och verksamhet som kan generera skada på annan säkerhetskänslig verksamhet.

Identifiera och bedöma skyddsvärden

3 § Verksamhetsutövaren ska identifiera vilka skyddsvärden som finns i den säkerhetskänsliga verksamheten, det vill säga

1. säkerhetsskyddsklassificerade uppgifter,
2. anläggningar, objekt, system, egendom och andra tillgångar som är av betydelse för Sveriges säkerhet, och
3. verksamhet som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.

4 § Verksamhetsutövaren ska bedöma från vilket eller vilka av perspektiven konfidentialitet, riktighet och tillgänglighet som de identifierade skyddsvärdena är skyddsvärda.

5 § Skyddsvärden som avses i 3 § första stycket 2 ska delas in i följande konsekvensnivåer utifrån en bedömning av den skada för Sveriges säkerhet en antagonistisk handling mot skyddsvärdet kan medföra:

– Synnerligen allvarlig skada för Sveriges säkerhet (nivå A).
– Allvarlig skada för Sveriges säkerhet (nivå B).
– Inte obetydlig skada för Sveriges säkerhet (nivå C).
– Endast ringa skada för Sveriges säkerhet (nivå D).

Säkerhetshot och dimensionerande antagonistiska förmågor

6 § Verksamhetsutövaren ska identifiera säkerhetshot kopplade till de identifierade skyddsvärdena och den säkerhetskänsliga verksamheten i stort.

7 § Säkerhetspolisen tillhandahåller, om Säkerhetspolisen inte bedömer att det i ett enskilt fall är olämpligt, beskrivningar av dimensionerande antagonistiska förmågor till verksamhetsutövare.

Tillsynsmyndigheten ska uppmärksamma Säkerhetspolisen på vilka av verksamhetsutövarna inom tillsynsmyndighetens tillsynsområde som har behov av beskrivningar av dimensionerande antagonistiska förmågor.

Sårbarheter

8 § Verksamhetsutövaren ska utifrån identifierade säkerhetshot och beskrivningen av dimensionerande antagonistiska förmågor, om Säkerhetspolisen har tillhandhållit en sådan, identifiera sårbarheter för respektive skyddsvärde och den säkerhetskänsliga verksamheten i stort.

Säkerhetsskyddsåtgärder

9 § Verksamhetsutövaren ska utifrån vad som framkommit vid identifiering och bedömning enligt 3–6 och 8 §§ bedöma vilka säkerhetsskyddsåtgärder som är nödvändiga.

Verksamhetsutövaren ska även dimensionera säkerhetsskyddsåtgärderna enligt 4 kap. 13 § samt 5 kap. 1 och 8–10 §§ utifrån en beskrivning av dimensionerande antagonistiska förmågor, om Säkerhetspolisen har tillhandahållit en sådan.

Beslut att fastställa säkerhetsskyddsanalysen

10 § Verksamhetsutövarens högsta chef eller motsvarande organ ska fastställa säkerhetsskyddsanalysen.

Redovisning av säkerhetsskyddsanalysen

11 § Verksamhetsutövaren ska på begäran lämna sin säkerhetsskyddsanalys till tillsynsmyndigheten respektive Säkerhetspolisen.

Upprättande av säkerhetsskyddsplan

12 § Efter att säkerhetsskyddsanalysen är fastställd ska verksamhetsutövaren upprätta en säkerhetsskyddsplan. Planen ska redogöra för hur behovet av säkerhetsskyddsåtgärder som identifierats i säkerhetsskyddsanalysen omhändertas. Det ska vidare framgå när åtgärderna ska vidtas och vilken funktion som ansvarar för dem.

Säkerhetsskyddsplanen ska fastställas av säkerhetsskyddschefen.

Särskild säkerhetsskyddsbedömning

13 § Av 4 kap. 7 § första stycket och 13 § första stycket säkerhetsskyddslagen (2018:585) samt 3 kap. 1 § säkerhetsskyddsförordningen (2021:955) följer att en verksamhetsutövare inför vissa förfaranden ska göra en särskild säkerhetsskyddsbedömning.

Verksamhetsutövaren ska i den särskilda säkerhetsskyddsbedömningen beskriva

1. vilka skyddsvärden som kan komma att påverkas av förfarandet och på vilket sätt,
2. vilka säkerhetshot som föreligger mot de påverkade skyddsvärdena och den säkerhetskänsliga verksamheten i stort,
3. vilka sårbarheter som föreligger för de påverkade skyddsvärdena och den säkerhetskänsliga verksamheten i stort samt hur sårbarheterna påverkas av förfarandet, och
4. vilka säkerhetsskyddsåtgärder som är nödvändiga som en följd av förfarandet.

I 3 kap. 1 § säkerhetsskyddsförordningen samt 4 kap. 3 § i dessa föreskrifter finns ytterligare bestämmelser om särskild säkerhetsskyddsbedömning inför driftsättning av informationssystem.

En särskild säkerhetsskyddsbedömning ska fastställas av säkerhetsskyddschefen eller den som han eller hon bestämmer.

Kontroll, uppföljning och åtgärdsplan

14 § Verksamhetsutövaren ska systematiskt

1. utvärdera om säkerhetsskyddsåtgärderna ger avsedd effekt,
2. identifiera brister och sårbarheter i säkerhetsskyddet, och
3. i övrigt kontrollera och följa upp att verksamheten följer regelverket för säkerhetsskydd.

Verksamhetsutövaren ska i en åtgärdsplan redovisa de åtgärder som behövs för att omhänderta avvikelser. I planen ska det anges vilken funktion som ansvarar för åtgärderna. Planen ska uppdateras löpande.

Hantering av säkerhetshotande händelser eller verksamhet

Rutiner, skademinimering och utvärdering

15 § Verksamhetsutövaren ska ha rutiner för hantering av säkerhetshotande händelser eller verksamhet som är av betydelse för den säkerhetskänsliga verksamheten.

16 § Verksamhetsutövaren ska vid säkerhetshotande händelser eller verksamhet, som är av betydelse för den säkerhetskänsliga verksamheten, vidta åtgärder så att skadlig inverkan på den säkerhetskänsliga verksamheten minimeras och så att den säkerhetskänsliga verksamheten så snart som möjligt kan återgå till normalläge.

17 § Verksamhetsutövaren ska utreda omständigheterna vid säkerhetshotande händelser eller verksamhet, som är av betydelse för den säkerhetskänsliga verksamheten, och utvärdera hanteringen av dem. Utifrån utvärderingen ska verksamhetsutövaren vidta nödvändiga åtgärder för att minimera skadeeffekten av liknande händelser i framtiden.

Anmälan

18 § För anmälan vid säkerhetshotande händelser eller verksamhet enligt 2 kap. 4 § säkerhetsskyddsförordningen (2021:955) ska blankett anvisad av Säkerhetspolisen användas.

Skadebedömning

19 § Vid en säkerhetshotande händelse eller verksamhet enligt 2 kap. 4 § första stycket 1 och 2 säkerhetsskyddsförordningen (2021:955) ska verksamhetsutövaren snarast, dock senast i samband med att anmälan görs till Säkerhetspolisen, påbörja arbetet med en skadebedömning.

Verksamhetsutövare utan utsedd säkerhetsskyddschef

20 § Om en säkerhetsskyddschef inte har utsetts med stöd av 2 kap. 7 § säkerhetsskyddslagen (2018:585) ska de beslut och uppgifter som ankommer på säkerhetsskyddschefen enligt dessa föreskrifter istället fattas och utföras av verksamhetsutövarens högsta chef eller motsvarande organ.

3 kap. Informationssäkerhet

Godkännande av informationssystem m.m.

1 § Säkerhetsskyddsklassificerade uppgifter i en viss säkerhetsskyddsklass får behandlas endast i informationssystem eller på lagringsmedium som verksamhetsutövaren godkänt för lägst den säkerhetsskyddsklass som uppgifterna har.

Krav på att uppmärksamma mottagaren på säkerhetsskyddsklassificeringen

2 § När en säkerhetskyddsklassificerad uppgift överlämnas ska mottagaren uppmärksammas på säkerhetsskyddsklassificeringen.

Rutiner

3 § Verksamhetsutövaren ska ha rutiner för behandling av säkerhetsskyddsklassificerade uppgifter och handlingar. Rutinerna ska reglera vad som gäller

för spårbarhet, upprättande, kopiering, utskrift, utdrag, kvittering, förvaring, distribution, medförande, inventering och förstöring.

Verksamhetsutövaren ska ha rutiner för behandling av uppgifter och handlingar som behöver skyddas utifrån ett riktighets- eller tillgänglighetsperspektiv.

Anteckningar

4 § En säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen konfidentiell eller högre ska, utöver en anteckning om vilken säkerhetsskyddsklass uppgifterna i handlingen har, i förekommande fall förses med en anteckning om handlingens beteckning, antal sidor och uppgift om bilagor.

5 § En säkerhetsskyddsklassificerad fysisk handling i säkerhetsskyddsklassen konfidentiell eller högre ska förses med en anteckning om handlingens exemplarnummer. I det allmännas verksamhet gäller kravet endast för allmänna handlingar.

6 § Om det beslutas att en säkerhetsskyddsklassificerad handling inte längre ska vara indelad i säkerhetsskyddsklass eller ska delas in i annan säkerhetsskyddsklass, ska detta antecknas på handlingen eller i ett register. Det ska av anteckningen framgå vem som har fattat beslutet och när det fattades.

7 § Om beslut som avses i 6 § innebär att en säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen kvalificerat hemlig inte längre ska vara indelad i säkerhetsskyddsklassen kvalificerat hemlig, ska beslutet fattas av verksamhetsutövarens högsta chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer. Om handlingen upprättats av någon annan än verksamhetsutövaren ska samråd ske med den som upprättat handlingen innan beslutet fattas. Anteckning om samrådet ska göras på handlingen.

Kopia och utdrag

8 § Kopia av eller utdrag ur en säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen kvalificerat hemlig får göras endast efter beslut av verksamhetsutövarens högsta chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer.

Förvaring

9 § En säkerhetsskyddsklassificerad handling ska vara under kontroll eller förvaras i ett förvaringsutrymme som verksamhetsutövaren har godkänt enligt 5 kap. 10 §.

Kraven i första stycket gäller inte om handlingen skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten.

Register över vissa säkerhetsskyddsklassificerade handlingar

10 § I ett register över säkerhetsskyddsklassificerade fysiska handlingar i säkerhetsskyddsklassen konfidentiell eller högre ska handlingarnas beteck-

ning, säkerhetsskyddsklass, antal exemplar och mottagare av respektive exemplar framgå.

För varje exemplar som förvaras hos verksamhetsutövaren ska det av registret framgå vem som har kvitterat exemplaret, när exemplaret har inventerats och om exemplaret har återlämnats, förkommit, arkiverats eller förstörts.

Märkning av lagringsmedium

11 § Lagringsmedium för säkerhetsskyddsklassificerade uppgifter ska märkas med säkerhetsskyddsklass och identifieringsuppgift. Om lagringsmediet är fast monterat i annan utrustning ska i stället utrustningen märkas.

Distribution

12 § Verksamhetsutövaren ska se till att nödvändiga säkerhetsskyddsåtgärder vidtas vid distribution av säkerhetsskyddsklassificerade uppgifter inom och utom verksamheten. En försändelse med en säkerhetsskyddsklassificerad fysisk handling i säkerhetsskyddsklassen konfidentiell eller högre, eller ett lagringsmedium som innehåller en handling i motsvarande nivå, ska sändas med en distributör som har godkänts av verksamhetsutövaren. Det ska kunna verifieras att försändelsen har levererats till mottagaren.

13 § Tillsynsmyndigheterna får i ett enskilt fall besluta att försändelser till och från utlandet med säkerhetsskyddsklassificerade handlingar får distribueras på annat sätt än genom Utrikesdepartementets kurirförbindelser.

Kvittering m.m.

14 § Den som tar emot en säkerhetsskyddsklassificerad fysisk handling i säkerhetsskyddsklassen konfidentiell eller högre ska kvittera mottagandet i ett register, en liggare eller på ett kvitto. I det allmännas verksamhet gäller kravet endast för allmänna handlingar.

När en säkerhetsskyddsklassificerad fysisk handling i säkerhetsskyddsklassen konfidentiell eller högre återlämnas, ska detta antecknas på kvittensen.

Verksamhetsutövaren ska bevara kvittensen i minst tio år. Om handlingen är kvalificerat hemlig ska kvittensen bevaras i minst 25 år. I det allmännas verksamhet tillämpas istället bestämmelserna om gallring i arkivlagen (1990:782) och föreskrifter som har meddelats med stöd av den lagen.

15 § Verksamhetsutövaren ska anteckna vem som är mottagare av en säkerhetsskyddsklassificerad elektronisk handling i säkerhetsskyddsklassen kvalificerat hemlig i handlingen eller i ett register.

16 § Vad som anges i 14 och 15 §§ gäller inte när arkiv-, expeditions-, sambands- eller tryckeripersonal tar emot en säkerhetsskyddsklassificerad handling för registrering, kopiering, distribution, arkivering eller förstöring, om inte den som lämnar över handlingen begär det. Vad som anges i 15 § gäller inte heller för personal som arbetar med drift av informationssystem när personalen hanterar lagringsmedium som har tilldelats eller ska tilldelas andra personer.

17 § Om uppgifter i en säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen kvalificerat hemlig lämnas muntligen eller genom visning, ska anteckning om detta göras i handlingen eller i ett register. Det ska av anteckningen framgå vem som har lämnat uppgifterna, när de har lämnats och till vem eller vilka de har lämnats.

Medförande utanför verksamhetsutövarens lokaler

18 § Om en säkerhetsskyddsklassificerad handling medförs till eller från verksamhetsutövarens lokaler ska den vara under kontroll eller förvaras i ett förvaringsutrymme som verksamhetsutövaren har godkänt enligt 5 kap. 10 §.

Kraven i första stycket gäller inte om handlingen skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten.

19 § Säkerhetsskyddschefen får i ett enskilt fall besluta att personal, som är behörig enligt 2 kap. 2 § säkerhetsskyddsförordningen (2021:955), får medföra en försändelse med en säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen hemlig eller lägre till utlandet.

20 § Verksamhetsutövarens högsta chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer får besluta att en säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen kvalificerat hemlig får medföras från verksamhetsutövarens lokaler.

Inventering

21 § Av 3 kap. 8 § säkerhetsskyddsförordningen (2021:955) följer att säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklassen kvalificerat hemlig ska inventeras minst en gång per år.

Inventering av säkerhetsskyddsklassificerade fysiska handlingar i säkerhetsskyddsklassen konfidentiell eller hemlig ska ske minst en gång per år.

Lagringsmedier som innehåller uppgifter i säkerhetsskyddsklassen konfidentiell eller högre ska inventeras minst en gång per år.

Förstöring

22 § Förstöring av säkerhetsskyddsklassificerade uppgifter ska ske så att uppgifterna inte kan återskapas.

23 § Förstöring av en säkerhetsskyddsklassificerad fysisk handling i säkerhetsskyddsklassen konfidentiell eller högre ska dokumenteras.

Avveckling eller återanvändning av lagringsmedium

24 § Verksamhetsutövaren ska ha rutiner för avveckling eller återanvändning av lagringsmedium som används i säkerhetskänslig verksamhet. Rutinerna ska säkerställa att information på lagringsmediet inte kan återskapas.

Granskning vid utveckling och anskaffning

1 § Verksamhetsutövaren ska se till att egenutvecklad programvara i informationssystem som har betydelse för säkerhetskänslig verksamhet granskas för att upptäcka och åtgärda säkerhetsbrister och sårbarheter.

2 § Verksamhetsutövaren ska se till att hårdvara och tredjepartsprogramvara i informationssystem som har betydelse för säkerhetskänslig verksamhet granskas för att upptäcka och åtgärda säkerhetsbrister och sårbarheter, eller att hårdvaran och programvaran på annat sätt bedöms vara tillförlitlig från säkerhetsskyddssynpunkt.

Åtgärder inför driftsättning eller förändring

3 § Verksamhetsutövaren ska, innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift, genomföra tester av skyddsåtgärderna. Resultatet ska jämföras med de säkerhetskrav som gäller för informationssystemet. Den särskilda säkerhetsskyddsbedömningen ska uppdateras med eventuella avvikelser och de kompensatoriska åtgärder som måste vidtas.

4 § Verksamhetsutövaren ska innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift, bedöma vilka resurser och kompetenser som krävs för att bibehålla fastställt säkerhetsskydd under informationssystemets förväntade livstid.

Rutiner för hantering av informationssystem

5 § Verksamhetsutövaren ska fastställa rutiner för hanteringen av informationssystem som har betydelse för säkerhetskänslig verksamhet under systemets förväntade livstid.

Granskning av säkerheten

6 § Verksamhetsutövaren ska årligen granska säkerheten i ett informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig eller i informationssystem som är av motsvarande betydelse för Sveriges säkerhet.

Unika identiteter och spårbarhet

7 § Alla utställda identiteter i ett informationssystem som har betydelse för säkerhetskänslig verksamhet ska vara unika över tid. Åtkomsten ska vara spårbar till individ, system eller resurs.

Behörighetsstyrning

8 § Verksamhetsutövaren ska tilldela behörigheter som ger systemadministrativ åtkomst eller annan särskild tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet restriktivt. Beslut om sådana behö-

righeter ska fattas av säkerhetsskyddschefen eller den han eller hon bestämmer. Behörigheterna ska vara tidsbegränsade, följas upp och omprövas löpande, minst årligen.

Autentisering m.m.

9 § Verksamhetsutövaren ska se till att autentisering vid åtkomst till informationssystem som har betydelse för säkerhetskänslig verksamhet baseras på flera faktorer, om det inte är uppenbart obehövligt.

10 § Verksamhetsutövaren ska fastställa tekniska eller administrativa regler för utformning, byte och hantering av lösenord, där sådana används för att ge åtkomst till informationssystem som har betydelse för säkerhetskänslig verksamhet.

11 § En anteckning med uppgift om lösenord som ger tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet ska vara under kontroll eller förvaras i ett förvaringsutrymme som verksamhetsutövaren enligt 5 kap. 10 § har godkänt för förvaring av säkerhetsskyddsklassificerade handlingar.

12 § Vid användning av en central funktion för identifiering eller behörighetskontroll, ska verksamhetsutövaren se till att denna funktion ges ett säkerhetsskydd som svarar upp mot det säkerhetsskydd som de anslutna informationssystemen ska ha.

Skydd mot röjande signaler

13 § Verksamhetsutövaren ska för ett informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre vidta åtgärder för att försvåra obehörig inhämtning av röjande signaler utifrån identifierade säkerhetshot och en beskrivning av dimensionerande antagonistiska förmågor, om Säkerhetspolisen tillhandahållit en sådan.

Kommunikationssäkerhet

14 § Verksamhetsutövaren ska se till att informationssystem som har betydelse för säkerhetskänslig verksamhet

1. kommunicerar på ett kontrollerat sätt med komponenter eller delsystem inom samma informationssystem, och
2. kommunicerar på ett kontrollerat sätt med informationssystem eller nätverk som inte omfattas av krav på säkerhetsskydd.

15 § Verksamhetsutövaren ska se till att informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat hemlig eller konfidentiell, logiskt separeras från informationssystem eller nätverk som inte omfattas av motsvarande krav på säkerhetsskydd.

16 § Verksamhetsutövaren ska se till att informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig, fysiskt separeras från informationssystem eller nätverk som inte omfattas av motsvarande krav på säkerhetsskydd.

17 § Informationssystem som är separerade från andra informationssystem enligt 15 eller 16 § får genom envägskommunikation överföra data för export till eller import från andra informationssystem.

Konfiguration, uppdatering och dokumentering

18 § Verksamhetsutövaren ska för informationssystem som har betydelse för säkerhetskänslig verksamhet tillämpa konfiguration som använder lämpliga säkerhetsfunktioner, stänger av funktioner som inte används och även i övrigt reducerar sårbarheter.

19 § Verksamhetsutövaren ska se till att programvara i informationssystem som har betydelse för säkerhetskänslig verksamhet hålls uppdaterad så att säkerhetsbrister och sårbarheter motverkas.

Om det finns särskilda skäl får verksamhetsutövaren besluta om undantag från kravet i första stycket.

20 § Verksamhetsutövaren ska ha dokumentation som visar logiska samband och inbördes beroenden mellan komponenter som används i informationssystem som har betydelse för säkerhetskänslig verksamhet.

21 § Verksamhetsutövaren ska för informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen kvalificerat hemlig, dokumentera vilken hård- och mjukvara som används i informationssystemet och deras inbördes beroenden.

Kraven i första stycket gäller även informationssystem som är av motsvarande betydelse för Sveriges säkerhet.

Skydd mot skadlig kod

22 § Verksamhetsutövaren ska för informationssystem som har betydelse för säkerhetskänslig verksamhet analysera behovet av och i förekommande fall besluta att använda de funktioner för skydd mot skadlig kod som är nödvändiga från säkerhetsskyddssynpunkt.

Skydd mot obehörig förändring av informationssystem

23 § Verksamhetsutövaren ska för informationssystem som har betydelse för säkerhetskänslig verksamhet vidta skyddsåtgärder som ger förmåga att försvåra och upptäcka obehörig förändring av informationssystemet och dess säkerhetsskydd.

24 § Verksamhetsutövaren ska förse ett informationssystem som har betydelse för säkerhetskänslig verksamhet och som kommunicerar med andra informationssystem, med funktioner för intrångsdetektering och intrångsskydd.

Säkerhetsloggning

25 § Verksamhetsutövaren ska logga händelser som kan påverka säkerheten i informationssystem som har betydelse för säkerhetskänslig verksamhet.

26 § Verksamhetsutövaren ska ha rutiner för loggning av händelser som kan påverka säkerheten i informationssystem som har betydelse för säkerhetskänslig verksamhet. Rutinerna ska omfatta hur verksamhetsutövaren ska kunna upptäcka skadlig inverkan, obehörig åtkomst eller påverkan, och funktionsstörningar. Rutinerna ska även omfatta vilka åtgärder som ska vidtas vid upptäckta händelser.

27 § För informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter ska loggningen omfatta användning och ändring av behörigheter med systemadministrativ åtkomst och av roller med särskild behörighet till informationssystemet.

28 § Verksamhetsutövaren ska bevara säkerhetsloggar i minst tio år. För ett informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen kvalificerat hemlig ska säkerhetsloggar bevaras i minst 25 år. I det allmännas verksamhet tillämpas i stället bestämmelserna om gallring i arkivlagen (1990:782) och föreskrifter som har meddelats med stöd av den lagen.

29 § Verksamhetsutövaren ska vidta åtgärder för att skydda säkerhetsloggar mot obehörig åtkomst, ändring eller förstöring.

Säkerhetsövervakning

30 § Verksamhetsutövaren ska använda funktioner för säkerhetsövervakning av informationssystem som är avsedda för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig.

Kraven i första stycket gäller även informationssystem av motsvarande betydelse för Sveriges säkerhet.

31 § Verksamhetsutövaren ska ha rutiner för säkerhetsövervakning enligt 30 §. Rutinerna ska omfatta vad som ska övervakas och vilken funktion som ansvarar för övervakningen. Rutinerna ska även omfatta vad som behövs i övrigt samt vilka åtgärder som ska vidtas vid upptäckta händelser.

32 § Verksamhetsutövaren ska för informationssystem som är skyddsvärda utifrån perspektiven riktighet eller tillgänglighet ha de rutiner och funktioner som krävs för att upprätthålla kontinuitet i den säkerhetskänsliga verksamheten. Verksamhetsutövaren ska för sådana informationssystem vidta åtgärder som säkerställer att informationssystemet kan återställas.

Kontroll av säkerhetskopior

33 § När säkerhetskopiering av säkerhetsskyddsklassificerade uppgifter eller uppgifter i övrigt som har betydelse för säkerhetskänslig verksamhet genomförs, ska verksamhetsutövaren regelbundet, minst en gång per år, kontrollera att uppgifterna på säkerhetskopiorna går att återskapa.

5 kap. Fysisk säkerhet

Åtgärder för att upptäcka, försvåra och hantera

1 § Verksamhetsutövaren ska utifrån identifierade säkerhetshot och en beskrivning av dimensionerande antagonistiska förmågor, om Säkerhetspolisen tillhandahållit en sådan,

1. använda personell bevakning, teknisk bevakning eller en kombination av dessa för att upptäcka obehörigt tillträde till eller skadlig inverkan på den säkerhetskänsliga verksamheten tidigt så att åtgärder för att försvåra och hantera ger avsedd effekt,
2. vidta försvårande åtgärder som fördröjer obehörigt tillträde till den säkerhetskänsliga verksamheten till dess att hanterande åtgärder hinner vidtas,
3. vidta försvårande åtgärder som reducerar skadlig inverkan på den säkerhetskänsliga verksamheten, och
4. se till att åtgärder kan vidtas för att hantera obehörigt tillträde till eller skadlig inverkan på den säkerhetskänsliga verksamheten.

Styrning av tillträde

2 § Verksamhetsutövaren ska styra tillträdet till eller inom områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs så att endast behöriga får tillträde. Rutiner ska finnas för tilldelning och förändring av behörigheter. Behöriga ska inte ges större tillträde än nödvändigt.

3 § Verksamhetsutövaren ska utfärda skriftligt tillstånd för besökare till eller inom områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs.

4 § Verksamhetsutövaren ska besluta på vilket sätt identitet och behörighet ska kontrolleras för tillträde till eller inom områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs.

Koder, kort och nycklar

5 § Kort, nycklar och anteckningar med uppgift om kod, som var för sig ger åtkomst till områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs, ska vara under kontroll eller förvaras i ett förvaringsutrymme som verksamhetsutövaren har godkänt enligt 10 §.

6 § Verksamhetsutövaren ska ha en förteckning över koder, kort och nycklar till områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs. Av förteckningen ska det framgå till vem de har lämnats och när de lämnades samt var reservkod eller reservnyckel förvaras. Det ska vidare framgå om och i så fall när återlämnande skett.

Hantering av föremål som är olämpliga från säkerhetsskyddssynpunkt

7 § Verksamhetsutövaren ska ha rutiner för att säkerställa att föremål som är olämpliga från säkerhetsskyddssynpunkt inte förs till eller inom områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs.

Elektronisk utrustning som kan möjliggöra obehörig avlyssning av samtal får inte medföras vid samtal som behandlar säkerhetsskyddsklassificerade uppgifter.

Skydd mot obehörig avlyssning av samtal

8 § Verksamhetsutövaren ska besluta om vilka utrymmen som är godkända för regelbundna samtal som behandlar säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre. Av beslutet ska framgå den högsta säkerhetsskyddsklass för de uppgifter som får samtalas om i utrymmet.

Ett sådant utrymme får godkännas endast om det är försett med eller omges av åtgärder för att försvåra obehörig avlyssning utifrån identifierade säkerhetshot och en beskrivning av dimensionerande antagonistiska förmågor, om Säkerhetspolisen tillhandahållit en sådan.

Skydd mot obehörig insyn

9 § Verksamhetsutövaren ska besluta om vilka utrymmen som är godkända för regelbunden behandling av säkerhetsskyddsklassificerade uppgifter. Av beslutet ska framgå den högsta säkerhetsskyddsklass för de uppgifter som får behandlas i utrymmet.

Ett sådant utrymme får godkännas endast om det är försett med eller omges av åtgärder för att försvåra obehörig insyn utifrån identifierade säkerhetshot och en beskrivning av dimensionerande antagonistiska förmågor, om Säkerhetspolisen tillhandahållit en sådan.

Förvaringsutrymmen

10 § Verksamhetsutövaren ska besluta om vilka förvaringsutrymmen som är godkända för förvaring av säkerhetsskyddsklassificerade handlingar samt

kort, nycklar och anteckningar med uppgift om kod, som var för sig ger åtkomst till områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs.

Ett förvaringsutrymme får godkännas endast om det är försett med eller omges av åtgärder för att upptäcka, försvåra och hantera obehörigt tillträde utifrån identifierade säkerhetshot och en beskrivning av dimensionerande antagonistiska förmågor, om Säkerhetspolisen tillhandahållit en sådan.

Beslut att godkänna ett förvaringsutrymme avsett för förvaring av säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklassen kvalificerat hemlig ska fattas av verksamhetsutövarens högsta chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer.

6 kap. Personalsäkerhet

Utbildning

1 § Verksamhetsutövaren ska säkerställa att den som ska delta i säkerhetskänslig verksamhet får relevant utbildning i säkerhetsskydd innan personen får åtkomst till den säkerhetskänsliga verksamheten. Sådan utbildning ska därefter ges regelbundet i den omfattning som behövs.

Verksamhetsutövaren ska se till att innehållet i de utbildningar som genomförs anpassas efter deltagarnas funktioner och ansvar i verksamheten. Utbildningarna ska framgå av en utbildningsplan.

Vem som deltagit i utbildningar ska dokumenteras. Av dokumentationen ska även tidpunkt för utbildningarna och utbildningarnas innehåll framgå.

Säkerhetsprövning

2 § Verksamhetsutövaren ska med utgångspunkt i säkerhetsskyddsanalysen föra förteckning över vilka anställningar eller annat deltagande i den säkerhetskänsliga verksamheten som placerats i säkerhetsklass eller som ska föregås av registerkontroll enligt 3 kap. 15 § säkerhetsskyddslagen (2018:585).

3 § Verksamhetsutövaren ska med utgångspunkt i säkerhetsskyddsanalysen besluta om och föra förteckning över vilka anställningar eller annat deltagande i den säkerhetskänsliga verksamheten som ska föranleda säkerhetsprövning utan placering i säkerhetsklass.

4 § Grundutredning enligt 5 kap. 2 § säkerhetsskyddsförordningen (2021:955) ska innehålla en säkerhetsprövningsintervju där lojalitet, pålitlighet och sårbarhet hos den som prövas bedöms.

Verksamhetsutövaren ska inom ramen för säkerhetsprövningen löpande under anställningen eller deltagandet göra dessa bedömningar.

5 § Uppgifter som framkommit vid säkerhetsprövningen och som behövs för att verksamhetsutövaren ska kunna följa upp säkerhetsprövningen under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår ska dokumenteras.

6 § Verksamhetsutövaren ska genomföra avslutande säkerhetssamtal när personens deltagande i den säkerhetskänsliga verksamheten upphör, om det inte är uppenbart obehövligt.

Registerkontroll och särskild personutredning

Ansökan

7 § Den som beslutar om placering i säkerhetsklass ska ansöka om registerkontroll och särskild personutredning på av Säkerhetspolisen anvisad blankett. Om anställningen eller deltagandet är tidsbegränsat ska tiden anges.

8 § Vid ansökan om registerkontroll i säkerhetsklass 1 eller vid ansökan efter beslut av regeringen enligt 5 kap. 12 § andra stycket säkerhetsskyddsförordningen (2021:955) ska regeringsbeslutet ligga till grund för ansökan och finnas tillgängligt hos verksamhetsutövaren.

9 § Ansökan om registerkontroll av personal hos en aktör som verksamhetsutövaren har ingått säkerhetsskyddsavtal med, får göras först när avtalet har anmälts till Säkerhetspolisen.

En ansökan om registerkontroll får innehålla hänvisning till endast ett säkerhetsskyddsavtal.

Dokumentation av samtycke

10 § Verksamhetsutövaren ska dokumentera att samtycke till registerkontroll och särskild personutredning har lämnats av den som säkerhetsprövningen gäller.

Kontrollorsak

11 § I ansökan om registerkontroll ska kontrollorsaken framgå tydligt. Kontrollorsaken ska övergripande beskrivas med vilken säkerhetskänslig verksamhet personen avses delta i och vilka skyddsvärden personen får tillgång till, som en följd av sitt deltagande.

Svar på ansökan om registerkontroll

12 § Svar på ansökan om registerkontroll ska lämnas till den som ansökt om registerkontrollen.

Om det vid registerkontrollen eller den särskilda personutredningen framkommit uppgifter som ska lämnas ut för säkerhetsprövning ska svaret istället lämnas till den som ska göra bedömningen enligt 3 kap. 4–4b §§ säkerhetsskyddslagen (2018:585).

Om en uppgift har lämnats ut för säkerhetsprövning ska den som beslutar om placering i säkerhetsklass och Säkerhetspolisen underrättas om den kontrollerade godkänts vid säkerhetsprövningen eller inte.

13 § Verksamhetsutövaren ska se till att en förnyad registerkontroll görs när någon som innehar en säkerhetsklassad befattning får en annan befattning som inte omfattas av tidigare kontrollorsak eller den befintliga befattningen blir placerad i en annan säkerhetsklass. Detsamma gäller, såvitt avser registerkontrollerade personer i säkerhetsklass 1 eller 2, om den kontrollerade ingått äktenskap eller inlett ett samboförhållande efter den senaste registerkontrollen.

Ändring av den kontrollerades förhållanden

14 § Verksamhetsutövaren ska se till att registerkontroll avseende make, maka eller sambo avslutas, såvitt avser registerkontrollerade personer i säkerhetsklass 1 eller 2, om den kontrollerades äktenskap har upplösts eller om samboförhållandet har upphört. Underrättelsen ska ske på av Säkerhetspolisen anvisad blankett.

Funktion som svarar för hantering av registerkontroller

15 § Den som beslutar om placering i säkerhetsklass ska ha en funktion som svarar för hanteringen av registerkontroller.

Kontaktuppgifter för sådan funktion ska redovisas till Säkerhetspolisen på av myndigheten anvisad blankett. Uppgifterna ska hållas uppdaterade gentemot Säkerhetspolisen.

7 kap. Skyldigheter när en annan aktör kan få tillgång till säkerhetskänslig verksamhet

Anmälan om säkerhetsskyddsavtal

1 § Anmälan enligt 6 kap. 5 § säkerhetsskyddsförordningen (2021:955) ska göras på blankett anvisad av Säkerhetspolisen.

Nivåer

2 § Ett säkerhetsskyddsavtal enligt 4 kap. 1 § säkerhetsskyddslagen (2018:585) ska ingås på någon av följande nivåer:

– Nivå 1: Om den andra aktören kommer att få tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre eller få tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet utanför verksamhetsutövarens områden, byggnader och andra anläggningar eller objekt.

– Nivå 2: Om den andra aktören kommer att få tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre eller få tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet inom verksamhetsutövarens områden, byggnader och andra anläggningar eller objekt.

– Nivå 3: Om den andra aktören kan komma att få tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre eller få tillgång till säkerhetskänslig verksamhet av motsvarande bety-

delse för Sveriges säkerhet inom verksamhetsutövarens områden, byggnader och andra anläggningar eller objekt.

3 § Vid samverkan eller samarbete mellan aktörer som bedriver säkerhetskänslig verksamhet kan ett säkerhetsskyddsavtal ingås mellan fler än två parter. Avtalet ska då ingås i en nivå som motsvarar den högsta nivå som hade gällt i fall parterna istället ingått bilaterala avtal.

Av 3 kap. 3 § första stycket säkerhetsskyddslagen (2018:585) följer att säkerhetsprövningen får göras mindre omfattande om det finns särskilda skäl. Vid samarbete eller samverkan enligt första stycket kan grundutredning, registerkontroll och särskild personutredning underlåtas för det fall personen i fråga redan är föremål för en säkerhetsprövning som omfattar samarbetet eller samverkan.

Godkännande av lokaler eller utrymmen

4 § En verksamhetsutövare som avser att ingå ett säkerhetsskyddsavtal i nivå 1 ska på plats inspektera motpartens säkerhetsskydd beträffande aktuella lokaler eller utrymmen. Verksamhetsutövaren får endast godkänna lokalerna eller utrymmena om kraven enligt säkerhetsskyddsavtalet kan tillgodoses.

Säkerhetsprövning och utbildning

5 § Verksamhetsutövaren ska med utgångspunkt i säkerhetsskyddsanalysen och den särskilda säkerhetsskyddsbedömningen bedöma vilka befattningar hos motparten som ska placeras i säkerhetsklass och vilka befattningar hos motparten som ska säkerhetsprövas utan placering i säkerhetsklass.

Bedömningen ska resultera i en förteckning och omfatta motpartens ledning, personal och övriga hos motparten som ska delta i den säkerhetskänsliga verksamheten.

6 § Verksamhetsutövaren ska säkerställa att personal hos en motpart som verksamhetsutövaren ingått säkerhetsskyddsavtal med har relevant kunskap inom säkerhetsskydd och tillräcklig kännedom om verksamhetsutövarens skyddsvärden för arbetet de ska utföra.

Säkerhetsskyddsinstruktion

7 § Verksamhetsutövaren ska, när ett säkerhetsskyddsavtal har ingåtts i nivå 1, säkerställa att motparten dokumenterar hur denna uppfyller kravet på säkerhetsskydd enligt avtalet i en säkerhetsskyddsinstruktion. Verksamhetsutövaren ska godkänna säkerhetsskyddsinstruktionen.

Kontroll av att motparten följer säkerhetsskyddsavtalet

8 § Verksamhetsutövaren ska under den tid förfarandet pågår kontrollera att motparten följer kraven enligt säkerhetsskyddsavtalet.

Vid säkerhetsskyddsavtal i nivå 1 ska verksamhetsutövaren regelbundet på plats kontrollera motpartens säkerhetsskydd beträffande aktuella lokaler eller utrymmen.

Vid samverkan eller samarbete mellan aktörer som bedriver säkerhetskänslig verksamhet kan det i säkerhetsskyddsavtalet regleras att respektive part ansvarar för att följa upp att den egna verksamheten uppfyller kraven på säkerhetsskydd enligt säkerhetsskyddsavtalet. Verksamhetsutövaren ska då kontrollera att motparten gjort en sådan uppföljning.

När säkerhetsskyddsavtalet upphört

9 § När ett säkerhetsskyddsavtal har upphört ska verksamhetsutövaren upplysa motparten om den tystnadsplikt som gäller för de säkerhetsskyddsklassificerade uppgifter som motparten har fått tillgång till genom förfarandet.

Motparten ska återlämna eller förstöra alla säkerhetsskyddsklassificerade handlingar enligt verksamhetsutövarens anvisningar.

Undantag vid samverkan eller samarbete mellan aktörer som bedriver säkerhetskänslig verksamhet

10 § Vid samverkan eller samarbete mellan aktörer som bedriver säkerhetskänslig verksamhet ska 4–7 §§, 8 § andra stycket och 9 § första stycket inte tillämpas.

Förfaranden som inte omfattas av krav på säkerhetsskyddsavtal

11 § En verksamhetsutövare som avser att genomföra en upphandling, ingå ett avtal eller inleda en samverkan eller ett samarbete med annan aktör som rör säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat hemlig eller säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet, ska säkerställa att säkerhetsskyddet regleras på något annat sätt än genom ett säkerhetsskyddsavtal.

Anmälan om samråd

12 § Till anmälan om samråd i förfaranden som kräver säkerhetsskyddsavtal enligt 4 kap. 7 § första stycket och 9 § säkerhetsskyddslagen (2018:585) ska bifogas verksamhetsutövarens särskilda säkerhetsskyddsbedömning, lämplighetsprövning och utkast till säkerhetsskyddsavtal. Anmälan ska vara undertecknad av verksamhetsutövaren, behörig ställföreträdare för denna eller ombud med fullmakt.

13 § Till anmälan om samråd inför överlåtelse av säkerhetskänslig verksamhet och viss egendom enligt 4 kap. 13 § första stycket och 15 § första stycket säkerhetsskyddslagen (2018:585) ska bifogas en beskrivning av den avsedda överlåtelsen jämte verksamhetsutövarens särskilda säkerhetsskyddsbedömning och lämplighetsprövning, inklusive information om förvärvaren och dennas ägarstruktur. Anmälan ska vara undertecknad av verksamhetsutövaren, behörig ställföreträdare för denna eller ombud med fullmakt.

14 § Till en anmälan om samråd inför överlåtelse av aktier eller andelar i säkerhetskänslig verksamhet enligt 4 kap. 15 § tredje stycket säkerhetsskyddslagen (2018:585) ska bifogas information om verksamhetsutövaren, inklusive

organisationsnummer och kontaktuppgifter, samt en beskrivning av den avsedda överlåtelsen, inklusive information om förvärvaren och i det fall förvärvaren är en juridisk person dennas ägarstruktur. Anmälan ska vara undertecknad av överlåtaren, behörig ställföreträdare för denna eller ombud med fullmakt.

8 kap. Överklagande och undantag från föreskrifterna

Överklagande

1 § Beslut enligt dessa föreskrifter får inte överklagas.

Undantag från föreskrifterna

2 § Säkerhetspolisen och tillsynsmyndigheterna får medge undantag från bestämmelserna i dessa föreskrifter.

Innan en tillsynsmyndighet fattar beslut om undantag enligt första stycket ska myndigheten samråda med Säkerhetspolisen.

---

1. Dessa föreskrifter träder i kraft den 1 mars 2022.

2. Genom föreskrifterna upphävs Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2).

3. Bestämmelserna i 2 kap. 1–6 samt 8 och 9 §§ behöver inte tillämpas på en säkerhetsskyddsanalys som har fastställts före den 1 mars 2022 till dess att säkerhetsskyddsanalysen ska uppdateras enligt 2 kap. 1 § andra stycket säkerhetsskyddsförordningen (2021:955).

4. Bestämmelserna i 3 kap. 5, 10, 14, 21 och 23 §§ behöver inte tillämpas på säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklassen konfidentiell förrän den 1 januari 2023.

5. Bestämmelsen i 6 kap. 12 § andra stycket ska inte tillämpas förrän den 1 januari 2023.

CHARLOTTE VON ESSEN

Carl Rundström
(Rättsenheten)