En ny säkerhetsskyddslag

- sett ur informationssäkerhetsperspektiv

Jimmy Arvidsson

2019-05-02

Säkerhetspolisen

Agenda

- Föreskriftsarbetet
- Generella krav
- Informationsklassificering
- Säkerhet i informationssystem

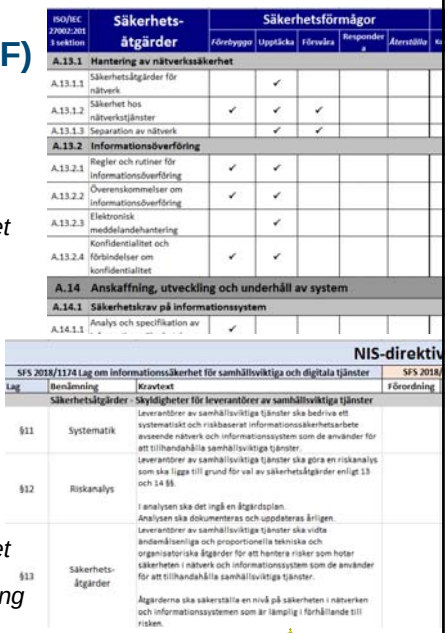
Säkerhetspolisen

FÖRESKRIFTSARBETET

Säkerhetspolisen

Säkerhetsförmågor (KSF)

- *Autentisering och behörighet*
- *Säkerhetsövervakning*
- *System- och informationsintegritet*
- *Skydd mot skadlig kod*
- *Säkerhetsförvaltning (underhåll)*
- *Intrångsskydd*
- *Tillgänglighet*
- *Incidenthantering*
- *Obehörig avlyssning*
- *Fysisk och miljörelaterad säkerhet*
- *Kompetens och personalförsörjning*



ISO/IEC 27002:2013 sektion	Säkerhets-åtgärder	Säkerhetsförmågor					
		Förebygga	Upptäcka	Försvåra	Responder a	Återställa	Ku
A.13.1	**Hantering av nätverkssäkerhet**						
A.13.1.1	Säkerhetsåtgärder för nätverk		✓				
A.13.1.2	Säkerhet hos nätverkstjänster	✓	✓	✓			
A.13.1.3	Separation av nätverk		✓	✓			
A.13.2	**Informationsöverföring**						
A.13.2.1	Regler och rutiner för informationsöverföring	✓	✓				
A.13.2.2	Överenskommelser om informationsöverföring	✓	✓				
A.13.2.3	Elektronisk meddelandehantering		✓				
A.13.2.4	Konfidentialitet och förbindelser om konfidentialitet	✓	✓				
A.14	**Anskaffning, utveckling och underhåll av system**						
A.14.1	**Säkerhetskrav på informationssystem**						
A.14.1.1	Analys och specifikation av	✓					

NIS-direktiv

SFS 2018/1174 Lag om informationssäkerhet för samhällsviktiga och digitala tjänster			SFS 2018/
Lag	Benämning	Kravtext	Förordning
	Säkerhetsåtgärder - Skyldigheter för leverantörer av samhällsviktiga tjänster		
§11	Systematik	Leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.	
§12	Riskanalys	Leverantörer av samhällsviktiga tjänster ska göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder enligt 13 och 14 §§. I analysen ska det ingå en åtgärdsplan. Analysen ska dokumenteras och uppdateras årligen.	
§13	Säkerhets-åtgärder	Leverantörer av samhällsviktiga tjänster ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken.	

CISCSC
NIST CRF

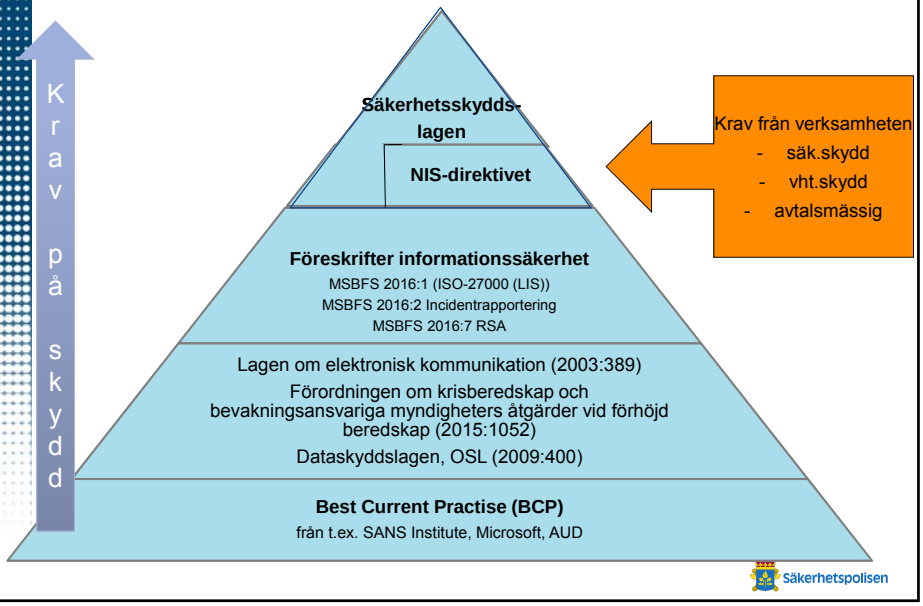
Säkerhetspolisen

Målbild för informationssäkerhet

- Avstämd förordning och föreskrifter med Försvarsmakten
- Tagit avstamp i:
  - Säkerhetspolisens tidigare arbeten
  - MSBFS 2016:1 - Föreskrifter inom informationssäkerhet för myndigheter
  - NIS-direktivet
  - Försvarsmaktens handböcker och regelverk
- Vad vi strävat efter att införa:
  - Systematiskt informationssäkerhet (regelverk)
    - Ledning, ansvar och kompens samt regelbunden uppföljning
  - Balanserat krav på fysiska och eletroniska handlingar
  - Säkerhetsförmågor istf säkerhetsfunktioner
    - Segmentering
    - Lagringsmedium
    - Sanitetsregler: inventariekontroll, härdning, intrångsövervakning, säkerhetsövervakning etc

Säkerhetspolisen

Hur det hänger samman



Säkerhetspolisen

GENERELLA KRAV

Säkerhetspolisen

Generella krav i lagen avseende informationssäkerhet

- Skyldigheter för den som bedriver säkerhetskänslig verksamhet
- Säkerhetsskyddsåtgärder
  - Informationssäkerhet
  - Fysisk säkerhet
  - Personalsäkerhet
- Säkerhetsskyddsklassificering
- Säkerhetsskyddsavtal
- Säkerhetsprövning
- Internationell säkerhetsskyddssamverkan och säkerhetsintyg

Säkerhetspolisen

Generella krav i förordningen avseende informationssäkerhet

- Säkerhetsskyddsanalys
- Säkerhetsskyddschef
- Behörighet att delta i säkerhetskänslig verksamhet
- Säkerhetsskyddsavtal
  - Upphandling
  - Internationell samarbete
  - Överlåtelse av säkerhetskänslig verksamhet
- Informationssäkerhet
- Fysisk säkerhet
- Personalsäkerhet
- Tillsyn, föreskrifter och rådgivning

Säkerhetspolisen

Generella krav i föreskrifterna avseende informationssäkerhet

- Säkerhetsskyddsanalys
- Säkerhetsskyddsplan
- Särskild säkerhetsskyddsbedömning
- Styrning av säkerhetsskyddsarbetet
  - Funktioner och ansvar
  - Regelverk
  - Skyldighet att säkerställa resurser och kompetenser
  - Styrning av åtkomst
  - Utbildning
  - Kontinuitet i säkerhetskänslig verksamhet
- Incidentanmälan
- Förbättringar, kontroll och uppföljning

Säkerhetspolisen

Incidentanmälan och rutiner, skademinimering och utvärdering

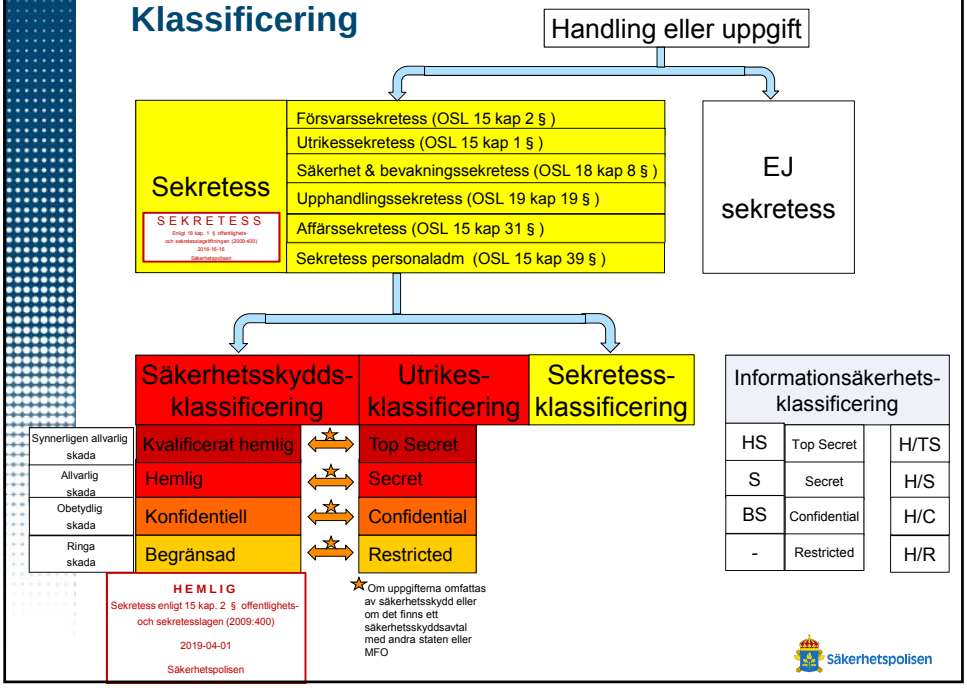
Benämning	Säkerhetsskyddslag (2018:585)	Säkerhetsskyddsförordning	Säkerhetsskyddsföreskrifter (PMFS 2019:2)			
INFORMATIONSSÄKERHET - incidenthantering			*Begränsat*	*Konfidentiellt*	*Hemlig*	*Kval.hemlig*
Rutiner, skade-minimering och utvärdering	Verksamhetsutövaren ska även kontrollera säkerhetsskyddet i den egna verksamheten, anmäla och rapportera sådant som är av vikt för säkerhetsskyddet och i övrigt vidta de åtgärder som krävs enligt denna lag. (2 kap 1§, 3 st)	En verksamhetsutövare ska skyndsamt anmäla till Säkerhetspolisen om 1. en säkerhetsskyddsklassificerad uppgift kan ha röjts, 2. det inträffat en it-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet, eller 3. verksamhetsutövaren får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet. Om verksamhetsutövaren tillhör Försvarsmaktens tillsynsområde enligt 7 kap. 1 § första stycket 1, ska anmälan göras också till Försvarsmakten. (2 kap 10§)	Verksamhetsutövaren ska ha rutiner för hantering av säkerhetshotande händelser som är av betydelse för verksamhetens säkerhetsskydd. (2 kap 20§)			
			Verksamhetsutövaren ska vid säkerhetshotande händelser som är av betydelse för verksamhetens säkerhetsskydd 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. (2 kap 21§)			
			Verksamhetsutövaren ska utvärdera inträffade säkerhetshotande händelser som är av betydelse för verksamhetens säkerhetsskydd. Utifrån utvärderingen ska verksamhetsutövaren införa de förbättringar som krävs för att minimera skadeeffekten av liknande händelser i framtiden. (2 kap 22§)			
Incident-anmälan		En verksamhetsutövare som är skyldig att anmäla säkerhetshotande händelser enligt 10 § första stycket 1 eller 2 och som tillhandahåller tjänster åt en annan verksamhetsutövare ska i samband med anmälan informera och vid behov samråda med de uppdragsgivare som berörs av incidenten. Vid anmälan enligt 10 § första stycket 1 eller 2 som rör säkerhetsskyddsklassificerade uppgifter som omfattas av ett internationellt säkerhetsskydds-åtagande enligt 6 kap. 1 §, ska Säkerhetspolisen underrätta den myndighet som är nationell säkerhetsmyndighet enligt det internationella säkerhetsskyddsåtagandet. (2 kap 11§)	Av 2 kap. 10 § första stycket säkerhetsskyddsförordningen (2018:658) framgår när en anmälan till Säkerhetspolisen om säkerhetshotande händelser och verksamhet ska göras. (2 kap 23§)			
			Om en säkerhetshotande händelse har inneburit en förlust av säkerhetsskyddsklassificerade uppgifter eller att uppgifterna kan ha röjts, ska verksamhetsutövaren snarast, dock senast i samband med att en anmälan om detta görs till Säkerhetspolisen, påbörja arbetet med en skadebedömning. (2 kap 24§)			
			Verksamhetsutövaren ska snarast, dock senast i samband med att en anmälan om en säkerhetshotande händelse görs till Säkerhetspolisen, överväga behovet av att informera andra verksamhetsutövare som från säkerhetsskyddssynpunkt kan vara berörda av händelsen. (2 kap 25§)			

Informationsklassificering

ATT SÄKERHETSKLASSIFICERA INFORMATION

Säkerhetspolisen

Klassificering



Säkerhetsskyddsklassificerade handlingar

- En verksamhetsutövare ska ha rutiner för behandling av säkerhetsskyddsklassificerade handlingar i säkerhetsskydds-klassen konfidentiell eller högre.
- Rutinerna ska reglera vad som gäller för:
  - spårbarhet,
  - upprättande,
  - kopiering,
  - utskrift,
  - utdrag,
  - kvittering,
  - förvaring,
  - distribution,
  - medförande och
  - destruktion samt
  - vad som behövs i övrigt.

Hanteringsregler

1. Mottagning, upprättande och diarieföring
2. Klassificering
3. Märkning
4. Exemplarnummer
5. Behörighet
6. Kvittenser
7. Visning
8. Förvaring
9. Gemensam användning
10. Kopiering och utskrift
11. Omklassificering
12. Distribution
13. Inventering
14. Avslut
15. Arkivering
16. Förstöring
17. Förlust och incidentanmälan
18. Utbildning

Säkerhetspolisen

Hantering av klassade handlingar

	Begränsat hemlig	Konfidentiell	Hemlig	Kvalificerat hemlig
Anteckning om säkerhetsskyddsklass	Ja	Ja (plus antal sidor och uppgift om bilagor)	Ja (plus antal sidor och uppgift om bilagor samt exemplarnummer för fysisk handling)	Ja (plus antal sidor och uppgift om bilagor samt exemplarnummer för fysisk handling)
Medgivande från högsta chef vid kopia eller utdrag	Nej	Nej	Nej	Ja
Förvaras av högsta chef	Nej	Nej	Nej	Ja
Märkning av lagringsmedium (säkerhetsskyddsklass och identifieringsuppgift)	Nej	Ja	Ja	Ja
Sänds med godkänd distributör	Nej	Ja	Ja	Ja
Anteckning om ursprungsland för handling som kan komma att lämnas ut till utlandet	Ja	Ja	Ja	Ja
Kvittering av fysisk handling*	Nej	Nej	Ja (i register, liggare eller särskilt kvitto). Bevaras i 10 år	Ja (på särskilt kvitto) Bevaras i 25 år
Anteckning om mottagare av elektronisk handling	Nej	Nej	Nej	Ja
Anteckning om muntlig delgivning eller visning	Nej	Nej	Nej	Ja
Tillstånd från högsta chef att medföra handling utanför verksamhetsutövarens lokaler	Nej	Nej	Nej	Ja
Årlig inventering av handlingar*	Nej	Nej	Ja (endast fysiska)	Ja
Årlig inventering av lagringsmedier	Nej	Nej	Ja	Ja
Dokumentering av förstöring av allmän handling	Nej	Nej	Ja	Ja

*För offentliga verksamhetsutövare gäller bestämmelsen endast för allmänna handlingar

Ackumulation och aggregation

Vid en skadebedömning av ett röjande av större informationsmängder behöver den sammantagna konsekvensen av att flera uppgifter röjs kan överstiga konsekvensen för om de enskilda uppgifterna röjs var och en för sig.

Frågan om uppgifterna kan sammanställas och korreleras påverkar konsekvenserna om uppgifterna skulle röjas och kan grovt sammanfattas i tre kategorier:

1. Varken mängd eller kombination av uppgifter förändrar konsekvensen
2. Större mängder av ***samma* uppgifter** ger sammantaget en något högre konsekvens. Detta kallas i denna promemoria för ***ackumulation***.
3. Större mängder av ***olika* uppgifter** kan sammanställas och korreleras. På så sätt får den aggregerade informationen större konsekvens om den skulle röjas. Konsekvensen av ett röjande ökar i detta fall oftast mer än i kategori 2 ovan. Detta kallas i denna promemoria för ***aggregation***.

Resonemanget är delvis baserat på Försvarsmaktens Handbok Sekretessbedömning Del A, 2011, avsnitt 4.3.4

Säkerhetspolisen

Säkerhet i informationssystem

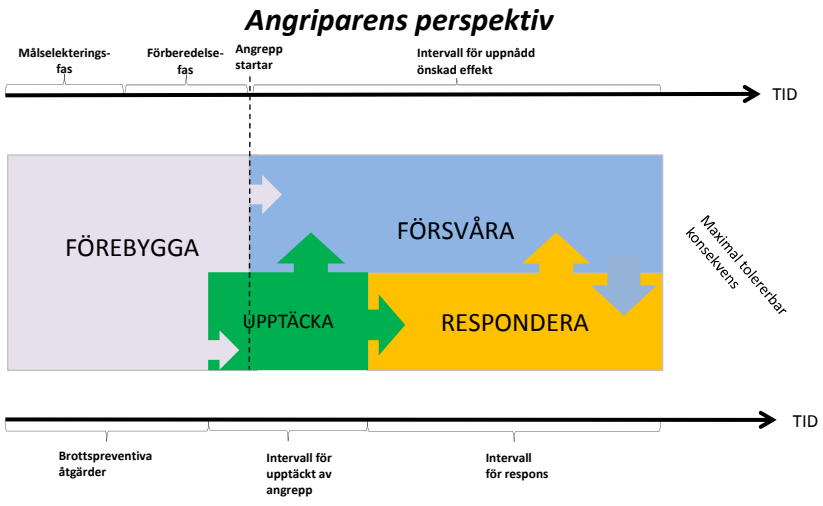
KRAV PÅ IT-SÄKERHET

Säkerhetspolisen

Säkerhetsskyddsförordning
Grundläggande krav - Informationssäkerhet

- Förberedande inför driftsättning
- Samråd (från konfidentiell)
- Driftgodkännande
- Lämpliga skyddsåtgärder för att
  - upptäcka, försvåra och hantera skadlig inverkan på informationssystem
  - skydda mot obehörig avlyssning av informationssystem
  - skydda mot obehörig åtkomst till och obehörigt nyttjade av informationssystem
- Spårbarhet av händelser som är av betydelse för säkerheten
- Skydd mot röjande signaler (från konfidentiell)
- Behandling av uppgifter utanför verksamhetsutövarens kontroll
- Fysisk säkerhet

Säkerhetspolisen



Säkerhetspolisen

Säkerhetsskyddsföreskriftens krav

Informationssystem som har betydelse för säkerhetskänslig verksamhet eller som hanterar säkerhetsskyddsklassificerade uppgifter eller information omfattas av krav på följande:

- Behandling i informationssystem
- Ny Kontinuerlig anpassning
- Ny Kompetens
- Åtgärder inför driftsättning eller förändring
- Granskning vid utveckling och anskaffning
- Rutiner för hantering av informationssystem
- Granskning av säkerheten
- Unika identiteter och spårbarhet
- Behörighetsstyrning
- Ny Autentisering
- Ny Konfiguration, uppdatering och dokumentering
- Skydd mot skadlig kod
- Intrångsdetektering och intrångsskydd
- Säkerhetsloggning
- Ny Säkerhetsövervakning
- Kommunikationssäkerhet
- Ny Separering
- Skydd mot röjande signaler
- Kontroll av säkerhetskopior
- Signalskydd

Säkerhetspolisen

Konfiguration, uppdatering och dokumentering (4 kap § § 23-26)

- Härdning
  - Stänga av de tjänster / funktioner som inte behövs
- Patchning och versionshantering
- System- och nätverksdokumentation
  - För att få kunskap och kopplingar, relationer och samband mellan system, applikationer, kommunikation etc
- Kontroll på tekniska komponenter
  - För att få kunskap om vilka tekniska komponenter som används

Säkerhetspolisen

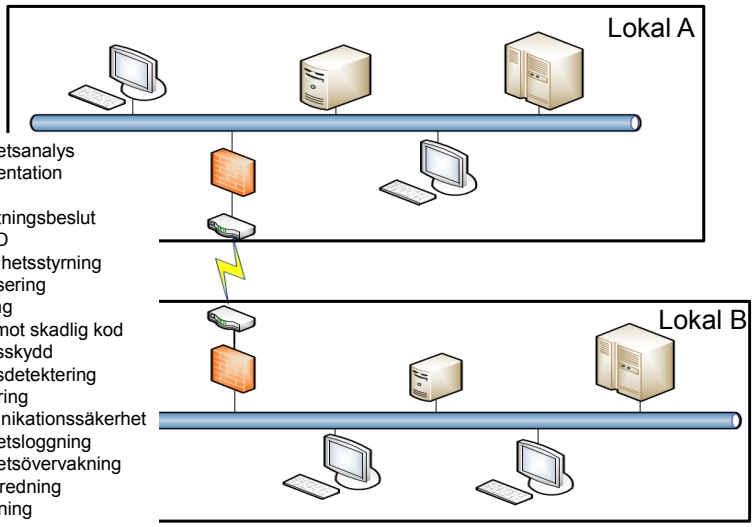
Autentisering

- Riktighet
  - Förmåga att försvåra och upptäcka obehörig förändring av informationssystem och dess säkerhetsskyddsåtgärder
- Autentisering
  - MFA
- Behörighetsstyrning
  - Restriktivitet med systemadministrativa eller motsvarande behörigheter
  - Tidsbegränsade och särskilt följas upp
- Kontinuerlig anpassning
  - Omvärldsbevakning, möta förändringar av hot och sårbarheter
- Säkerhetsövervakning
  - Funktioner och rutiner - vad som övervakas, av vem samt, när samt vilka åtgärder som ska vidtas

Säkerhetspolisen

Säkerhetsskyddsåtgärder Informationssystem med HEMLIGA uppgifter

1. Säkerhetsanalys
2. Dokumentation
3. Rutiner
4. Driftsättningsbeslut
5. Unika ID
6. Behörighetsstyrning
7. Autentisering
8. Härdning
9. Skydd mot skadlig kod
10. Intrångsskydd
11. Intrångsdetektering
12. Separering
13. Kommunikationssäkerhet
14. Säkerhetsloggning
15. Säkerhetsövervakning
16. RÖS-utredning
17. Granskning



Säkerhetspolisen

Informationssäkerhet – Kommunikationssäkerhet och Separation

Kommunikations-säkerhet	Verksamhetsutövaren ska se till att informationssystem som har betydelse för säkerhetskänslig verksamhet • kommunicerar på ett kontrollerat sätt med komponenter eller delsystem inom samma informationssystem, och • kommunicerar på ett kontrollerat sätt med informationssystem eller nätverk som inte omfattas av krav på säkerhetsskydd. (4 kap 19§)			
	Begränsat	**Konfidentiellt**	**Hemlig**	**Kval.hemlig**
Separering	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. (4 kap 20§)		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. Informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig, ska tillåta endast envägskommunikation vid import respektive export av data. (4 kap 21§)	

Säkerhetspolisen

Frågor ??

- Annars ….
- TACK för att ni lyssnat

- Kontaktuppgifter

Jimmy Arvidsson

Jimmy.arvidsson@sakerhetspolisen.se

010-568 7055

Säkerhetspolisen