Läsanvisningar IT-säkerhet:
Tabellen är tänkt att presentera krav på IT-säkerhet gällande skydd av säkerhetsskyddsklassificerade uppgifter och information samt krav på säkerhetskänslig verksamhet där skadlig inverkan kan medföra inverkan på Sveriges säkerhet.

I tabellen redovisas kraven per säkerhetsskyddsklass. Sträcker sig kravet över flera kolumner innebär detta att kravet är generellt och gäller samtliga säkerhetsskyddsklasser

Benämning	Säkerhetsskyddslagen (2018:585)			
	Begränsat	**Konfidentiellt**	**Hemlig**	**Kval.hemlig**
Skyldigheter för den som bedriver säkerhetskänslig verksamhet	Den som bedriver säkerhetskänslig verksamhet ska **utreda behovet av säkerhetsskydd** (säkerhetsskyddsanalys). Säkerhetsskyddsanalysen ska **dokumenteras.** Med utgångspunkt i analysen ska verksamhetsutövaren **planera och vidta de säkerhetsskyddsåtgärder som behövs** med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter. 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. Så långt det är möjligt ska säkerhetsskyddsåtgärderna utformas så att de inte medför någon skada eller annan olägenhet för andra allmänna eller enskilda intressen. (2 kap 1§)			
Säkerhetsskydds-åtgärder	**Informationssäkerhet** ska 1. förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och 2. förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet. (2 kap 2§)			
	Fysisk säkerhet ska 1.förebygga att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där säkerhetskänslig verksamhet i övrigt bedrivs, och 2. förebygga skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt som avses i 1. (2 kap 3§)			

	Personalsäkerhet ska 1. förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av någon annan anledning är säkerhetskänslig, och 2. säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd. (2 kap 4§)
Säkerhetsskydds-klassificering	Säkerhetsskyddsklassificerade uppgifter ska delas in i säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Indelningen i säkerhetsskyddsklasser ska göras enligt följande: 1.kvalificerat hemlig vid en synnerligen allvarlig skada, 2.hemlig vid en allvarlig skada, 3.konfidentiell vid en inte obetydlig skada, eller 4.begränsat hemlig vid endast ringa skada. Säkerhetsskyddsklassificerade uppgifter som omfattas av ett internationellt åtagande om säkerhetsskydd ska på motsvarande sätt delas in i säkerhetsskyddsklass, om de inte redan har klassificerats av en annan stat eller en mellanfolklig organisation. Indelningen i säkerhetsskyddsklass ska i sådant fall göras utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation. (2 kap 5§)
Säkerhetsskydds-avtal	Statliga myndigheter, kommuner och landsting som avser att genomföra en upphandling och ingå ett avtal om varor, tjänster eller byggentreprenader ska se till att det i ett säkerhetsskyddsavtal anges hur kraven på säkerhetsskydd enligt 1 § ska tillgodoses av leverantören om 1. det i upphandlingen förekommer säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller 2. upphandlingen i övrigt avser eller ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet. Verksamhetsutövaren ska kontrollera att leverantören följer säkerhetsskyddsavtalet. Det som anges i första och andra styckena gäller även för enskilda verksamhetsutövare som ingår avtal om varor, tjänster och byggentreprenader med utomstående leverantörer. (2 kap 6§)
Säkerhetsprövning	Den som genom en anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas. (3 kap 1§)

Säkerhetsskyddsförordningen (2018:658)

Benämning	Begränsat	Konfidentiellt	Hemlig	Kval.hemlig
Förberedande inför driftsättning	Innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift ska verksamhetsutövaren genom en särskild säkerhetsbedömning ta ställning till vilka säkerhetskrav i systemet som är motiverade och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses. Säkerhetsbedömningen ska dokumenteras. (3 kap 1§)			
Samråd		Innan ett informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre tas i drift, eller i väsentliga avseenden förändras, ska verksamhetsutövaren skriftligen samråda med Säkerhetspolisen. Om verksamhetsutövaren hör till Försvarsmaktens tillsynsområde enligt 7 kap. 1 § första stycket 1, ska denne i stället samråda med Försvarsmakten. Samrådsskyldigheten gäller även i fråga om andra informationssystem än sådana som anges i första stycket, om obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig. (3 kap 2§)		
Driftgodkännande	Ett informationssystem som ska användas i säkerhetskänslig verksamhet får inte tas i drift förrän det har godkänts från säkerhetsskyddssynpunkt av verksamhetsutövaren. Godkännandet ska dokumenteras. (3 kap 3§)			
Förmåga att upptäcka, försvåra och hantera samt spårbarhet	En verksamhetsutövare som ansvarar för ett informationssystem som ska användas i säkerhetskänslig verksamhet ska vidta lämpliga skyddsåtgärder för att kunna upptäcka, försvåra och hantera skadlig inverkan på informationssystemet samt obehörig avlyssning av, åtkomst till och nyttjande av informationssystemet. Verksamhetsutövaren ska också se till att spårbarhet finns för händelser som är av betydelse för säkerheten i systemet. (3 kap 4§)			
Skydd mot röjande signaler		En verksamhetsutövare som ansvarar för ett informationssystem enligt första stycket ska beakta risken för röjande signaler och vidta lämpliga skyddsåtgärder för systemet om 1.informationssystemet avses behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller 2. obehörig åtkomst till informationssystemet kan medföra en skada för Sveriges säkerhet som inte är obetydlig. (3 kap 4§)		

Utanför VU kontroll	Innan säkerhetsskyddsklassificerade uppgifter behandlas i ett informationssystem utanför verksamhetsutövarens kontroll ska denne försäkra sig om att säkerhetsskyddet för uppgifterna i systemet är tillräckligt. Om säkerhetsskyddsklassificerade uppgifter ska kommuniceras till ett informationssystem utanför verksamhetsutövarens kontroll ska uppgifterna skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten. (3 kap 5§)			
Undantag	Säkerhetspolisen och Försvarsmakten får inom respektive myndighets tillsynsområde meddela föreskrifter om undantag från kraven i 4 § första stycket (dvs förmåga att upptäcka, försvåra och hantera samt spårbarhet) Försvarsmakten får om det finns särskilda skäl också besluta om undantag från kraven i 5 § andra stycket (dvs Försvarsmakten godkänd kryptering). Försvarsmakten ska samråda med Säkerhetspolisen innan ett beslut om undantag meddelas om det gäller verksamhet som hör till Säkerhetspolisens tillsynsområde och med Regeringskansliet (Utrikesdepartementet) om kravet följer av ett internationellt säkerhetsskyddsåtagande. (3 kap 6§)			
Fysisk säkerhet	Områden, byggnader och andra anläggningar eller objekt där säkerhetsskyddsklassificerade uppgifter förvaras eller annars behandlas, eller där säkerhetskänslig verksamhet i övrigt bedrivs, ska vara försedda med funktioner för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan utifrån ett identifierat säkerhetsskyddsbehov. (4 kap 1§)			
Benämning	**Säkerhetsskyddsföreskrifter (PMFS 2019:2)**			
	Begränsat	**Konfidentiellt**	**Hemlig**	**Kval.hemlig**
Säkerhets-skyddsanalys	Den som bedriver säkerhetskänslig verksamhet ska enligt 2 kap. 1 § säkerhetsskyddslagen (2018:585) göra en säkerhetsskyddsanalys. Säkerhetsskyddsanalysen innebär att säkerhetsskyddsklassificerade uppgifter och vad som i övrigt behöver ett säkerhetsskydd ska identifieras. Vilka delar av verksamheten som är skyddsvärda med hänsyn till Sveriges säkerhet samt vilka hot och sårbarheter som finns kopplade till detta skyddsvärde ska också identifieras. Säkerhetsskyddsanalysen ska även innehålla en bedömning av vilka säkerhetsskyddsåtgärder som är nödvändiga. Analysen ska hållas uppdaterad. (2 kap 1§)			
Säkerhetsskydds-chef	Vid verksamhet som förordningen gäller för ska det, om det inte är uppenbart obehövligt, finnas en säkerhetsskyddschef som kontrollerar att verksamheten bedrivs i enlighet med vad som föreskrivs i säkerhetsskyddslagen (2018:585) och denna förordning. Vid myndigheter ska säkerhetsskyddschefen vara direkt underställd myndighetens chef. (2 kap 2§)			

Behörighet att delta i verksamhet	Behörig att ta del av säkerhetsskyddsklassificerade uppgifter eller i övrigt delta i säkerhetskänslig verksamhet är, om inte något annat följer av bestämmelser i lag, endast den som 1. har bedömts pålitlig från säkerhetssynpunkt, 2. har tillräckliga kunskaper om säkerhetsskydd, och 3. behöver uppgifterna eller annan tillgång till verksamheten för att kunna utföra sitt arbete (2 kap 3§)
Sekretess- och tystnadsplikt	En verksamhetsutövare ska upplysa den som tillåts ta del av säkerhetsskyddsklassificerade uppgifter om räckvidden och innebörden av den sekretess och tystnadsplikt som följer av offentlighets- och sekretesslagen (2009:400) respektive 5 kap. 2 § säkerhetsskyddslagen (2018:585).
Funktioner och ansvar	Verksamhetsutövaren ska inrätta de funktioner för säkerhetsskyddsarbetet som behövs för att säkerställa att arbetet kan bedrivas på ett fullgott sätt, systematiskt och kontinuerligt samt att det kan kontrolleras och följas upp. (2 kap 13§)
	Verksamhetsutövaren ska se till att ansvaret för säkerhetsskyddsarbetet är tydligt definierat och kommunicerat till berörda funktioner. Verksamhetsutövaren ska se till att funktioner som kan representera motstående intressen i säkerhetsskyddsfrågor är separerade från varandra. (2 kap 14§)
Regelverk	Verksamhetsutövaren ska ha ett dokumenterat regelverk för att upprätthålla verksamhetens säkerhetsskydd. Verksamhetsutövaren ska genom regelverket: • klargöra ledningens och övriga funktioners ansvar för verksamhetens säkerhetsskydd, • säkerställa att de funktioner som ska arbeta med verksamhetens säkerhetsskydd har nödvändiga befogenheter, och • se till att säkerhetsskyddsarbetet bedrivs samordnat samt att det utvecklas löpande och utvärderas regelbundet. (2 kap 15§)
Plan för resurser och kompetens	Verksamhetsutövaren ska säkerställa att det finns resurser och kompetenser tillgängliga i den utsträckning som krävs för att upprätthålla säkerhetsskyddet. (2 kap 16§)
Styrning av åtkomst	Verksamhetsutövaren ska ha rutiner för tilldelning och förändring av behörigheter, fysiska eller elektroniska nycklar eller annat som ger åtkomst till säkerhetskänslig verksamhet. Verksamhetsutövaren ska kunna följa upp vilken åtkomst den som deltar i säkerhetskänslig verksamhet har till verksamheten, och regelbundet, minst en gång per år, ompröva sådana åtkomster. (2 kap 17§)

Utbildning	Verksamhetsutövaren ska ge den som deltar i säkerhetskänslig verksamhet relevant utbildning i säkerhetsskydd innan personen får åtkomst till verksamheten. Sådan utbildning ska därefter ges regelbundet i den omfattning som behövs. Verksamhetsutövaren ska utifrån säkerhetsskyddsanalysen se till att innehållet i de utbildningar som genomförs anpassas efter deltagarnas funktioner och ansvar i verksamheten. Utbildningarna ska framgå av en utbildningsplan. (2 kap 18§)
Kontinuitet	Verksamhetsutövaren ska ha rutiner och funktioner för att upprätthålla kontinuitet i säkerhetskänslig verksamhet om en funktionsstörning kan medföra mer än ringa skada för Sveriges säkerhet. Rutinerna ska utformas och tillämpas på sådant sätt att säkerhetsskyddet så långt det är möjligt bibehålls på motsvarande nivå som under normala förhållanden. Verksamhetsutövaren ska regelbundet utbilda i, utvärdera och vid behov uppdatera sådana rutiner som avses i första stycket. (2 kap 19§)
Förbättringar, kontroll och uppföljning	Verksamhetsutövaren ska regelbundet • utvärdera om säkerhetsskyddsåtgärderna ger avsedd effekt, • identifiera brister och sårbarheter i säkerhetsskyddet och genomföra förbättringar, • kontrollera och följa upp det säkerhetsskyddsarbete som bedrivs på uppdrag av verksamhetsutövaren hos externa aktörer, och • i övrigt kontrollera och följa upp att verksamheten följer regelverket för säkerhetsskydd. Verksamhetsutövaren ska dokumentera åtgärderna i en plan som ska uppdateras löpande. I planen ska det anges vilken funktion som är ansvarig för åtgärderna. (2 kap 26§)
Behandling i informations-system	Säkerhetsskyddsklassificerade uppgifter i en viss säkerhetsskyddsklass får behandlas endast i informationssystem eller på lagringsmedium som verksamhetsutövaren godkänt för lägst den säkerhetsskyddsklass som uppgifterna har. (3 kap 1§)
Rutiner	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 destruktion samt vad som behövs i övrigt för att upprätthålla ett fullgott säkerhetsskydd. Verksamhetsutövaren ska ha rutiner för behandling av uppgifter som behöver skyddas från ett tillgänglighets- eller riktighetsperspektiv. (3 kap 3§)
Kontinuerlig anpassning	Verksamhetsutövaren ska kontinuerligt anpassa säkerhetsskyddsåtgärder i informationssystem för att möta förändringar av hot och sårbarheter. Verksamhetsutövaren ska även fastställa hur detta ska genomföras och vem som ansvarar för att identifiera förändringarna. (4 kap 2§)

Kompetens	Verksamhetsutövaren ska se till att den som deltar i utveckling, framtagning av arkitektur, testning och drift av informationssystem som har betydelse för säkerhetskänslig verksamhet har tillräcklig kompetens avseende informationssäkerhet och sårbarheter i aktuellt informationssystem. (4 kap 3§)
Granskning vid utveckling och anskaffning	Verksamhetsutövaren ska se till att egenutvecklad programvara i informationssystem som har betydelse för säkerhetskänslig verksamhet granskas för att upptäcka och åtgärda säkerhetsbrister och sårbarheter. (4 kap 4§) Verksamhetsutövaren ska se till att tredjepartsprogramvara i informationssystem som har betydelse för säkerhetskänslig verksamhet granskas för att upptäcka och åtgärda säkerhetsbrister och sårbarheter, eller att programvaran på annat sätt bedöms vara tillförlitlig från säkerhetsskyddssynpunkt. (4 kap 5§)
Åtgärder inför driftsättning eller förändring	Verksamhetsutövaren ska vid en särskild säkerhetsskyddsbedömning enligt 3 kap. 1 § säkerhetsskyddsförordningen (2018:658), beakta såväl de enskilda säkerhetsskyddsklassificerade uppgifterna som den totala mängden sådana uppgifter som kan komma att behandlas i informationssystemet. (4 kap 6§) Verksamhetsutövaren ska, innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift, genomföra tester av säkerhetsskyddsåtgärderna. Resultatet ska dokumenteras och jämföras med de säkerhetskrav som gäller för informationssystemet. Den särskilda säkerhetsskyddsbedömningen ska uppdateras med eventuella avvikelser och de kompensatoriska åtgärder som måste vidtas. (4 kap 7§) Verksamhetsutövaren ska innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift, dokumentera vilka resurser och kompetenser som krävs för att bibehålla fastställt säkerhetsskydd under informationssystemets förväntade livstid. (4 kap 8§) Verksamhetsutövaren ska, innan samråd enligt 3 kap. 2 § säkerhetsskyddsförordningen (2018:658) sker med Säkerhetspolisen, kontrollera och dokumentera att de säkerhetskrav som identifierats i den särskilda säkerhetsskyddsbedömningen har implementerats och att säkerhetsskyddsåtgärderna ger avsedd effekt. (4 kap 9§)
Rutiner för hantering av informations-system	Verksamhetsutövaren ska fastställa rutiner för hanteringen av informationssystem som har betydelse för säkerhetskänslig verksamhet under systemets förväntade livstid. (4 kap 10§)

Granskning av säkerheten	Verksamhetsutövaren ska årligen granska säkerheten i informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig eller i informationssystem där en incident kan medföra allvarlig eller synnerligen allvarlig skada för Sveriges säkerhet. (4 kap 11§)
Unika identiteter och spårbarhet	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.
Behörighets-styrning	Verksamhetsutövaren ska tilldela sådana behörigheter som ger systemadministrativ åtkomst eller annan särskild tillgång till informationssys- tem som har betydelse för säkerhetskänslig verksamhet restriktivt. Behörigheterna ska vara tidsbegränsade och följas upp särskilt. Tilldelning av behörigheter enligt första stycket som inte direkt kan kopplas till någon fysisk individ ska ske särskilt restriktivt och beslutas av säkerhetsskyddschefen eller den han eller hon bestämmer. (4 kap 13§)
Autentisering	Verksamhetsutövaren ska se till att autentisering vid åtkomst till informationssystem som har betydelse för säkerhetskänslig verksamhet baseras på flera faktorer (*flerfaktorsautentisering*). (4 kap 14§)
	Verksamhetsutövaren ska fastställa tekniska eller administrativa regler för utformning, byte och hantering av lösenord, om sådana används för att ge tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet. Reglerna ska bl.a. innehålla bestämmelser om återanvändning av lösenord samt lösenordens längd och komplexitet. (4 kap 15§)
	Verksamhetsutövaren ska ge kod eller lösenord som ger tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet ett säkerhetsskydd som motsvarar det säkerhetsskydd som informationssystemet ska ha enligt skyddsdimensioneringen. (4 kap 16§)
	Vid användning av central funktion för identifiering eller behörighetskontroll, ska verksamhetsutövaren se till att denna funktion ges ett säkerhetsskydd som motsvarar det högsta säkerhetsskydd som de anslutna informationssystemen ska ha enligt skyddsdimensioneringen. (4 kap 17§)
Skydd mot röjande signaler	I 3 kap. 4 § andra stycket säkerhetsskyddsförordningen (2018:658) finns bestämmelser om skyddsåtgärder mot röjande signaler. Verksamhetstövaren ska besluta om sådana åtgärder. (4 kap 18§)

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§)	
Kryptering	Verksamhetsutövaren ska analysera behovet av användning av kryptografiska funktioner till skydd för säkerhetsskyddsklassificerade uppgifter och uppgifter som behöver skyddas från ett riktighetsperspektiv. I 3 kap. 5 § andra stycket säkerhetsskyddsförordningen (2018:658) finns bestämmelser om användning av kryptografiska funktioner som har godkänts av Försvarsmakten. (4 kap 22§)			

Konfiguration, uppdatering och dokumentering	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. (4 kap 23§)	
	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. (4 kap 24§)	
	Verksamhetsutövaren ska ha dokumentation som visar logiska samband och inbördes beroenden mellan komponenter som används i informationssystem som har betydelse för säkerhetskänslig verksamhet. (4 kap 25§)	
		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 där en incident kan medföra synnerligen allvarlig skada för Sveriges säkerhet. (4 kap 26§)
Skydd mot skadlig kod	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. (4 kap 27§)	
Riktighet	Verksamhetsutövaren ska för informationssystem som har betydelse för säkerhetskänslig verksamhet vidta säkerhetsskyddsåtgärder som ger förmåga att försvåra och upptäcka obehörig förändring av informationssystemet och dess säkerhetsskydd. (4 kap 28§)	

	Begränsat	Konfidentiellt	Hemlig	Kval.hemlig
Intrångs-detektering och intrångsskydd		Verksamhetsutövaren ska förse ett informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre och som kommunicerar med andra informationssystem, med funktioner för intrångsdetektering och intrångsskydd. (4 kap 29§)		
		Verksamhetsutövaren ska förse ett informationssystem där en incident kan medföra mer än ringa skada för Sveriges säkerhet och som kommunicerar med andra informationssystem, med funktioner för intrångsdetektering och intrångsskydd. (4 kap 30§)		
Säkerhets-loggning	Verksamhetsutövaren ska logga händelser som kan påverka säkerheten i informationssystem som har betydelse för säkerhetskänslig verksamhet (*säkerhetsloggning*). (4 kap 31§)			
	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 eller obehörig åtkomst eller påverkan samt funktionsstörningar. Rutinerna ska även omfatta vad som behövs i övrigt samt vilka åtgärder som ska vidtas vid upptäckta händelser. (4 kap 32§)			
	För informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter ska rutinerna omfatta loggning av användning och ändring av behörigheter med systemadministrativ åtkomst och av roller med särskild behörighet i informationssystemet. (4 kap 33§)			
	Verksamhetsutövaren ska bevara säkerhetsloggar i minst 10 år. För informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen kvalificerat hemlig ska säkerhetsloggar bevaras i minst 25 år. (4 kap 34§)			Verksamhetsutövaren ska bevara säkerhetsloggar i minst 10 år. För informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen kvalificerat hemlig ska säkerhetsloggar bevaras i minst 25 år. (4 kap 35§)
	Verksamhetsutövaren ska vidta åtgärder för att skydda säkerhetsloggar mot obehörig åtkomst, ändring eller förstöring. (4 kap 35§)			

	Begränsat	Konfidentiellt	Hemlig	Kval.hemlig
Säkerhets-övervakning			Verksamhetsutövaren ska använda funktion för säkerhetsövervakning av informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig. Kraven i första stycket gäller även informationssystem där en incident kan medföra allvarlig eller synnerligen allvarlig skada för Sveriges säkerhet. (4 kap 36§)	
			Verksamhetsutövaren ska ha rutiner för säkerhetsövervakning enligt 36 §. Rutinerna ska omfatta vad som ska övervakas och vem som ansvarar för övervakningen. Rutinerna ska även omfatta vad som behövs i övrigt samt vilka åtgärder som ska vidtas vid upptäckta händelser. (4 kap 37§)	
Kontroll av säkerhets-kopior	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. (4 kap 38§)			