Myndigheten för civilt försvars författningssamling

Utgivare: Anna Asp
ISSN 3119-2394

MCFFS
Remissutgåva
[Fyll i nr]
Utkom från trycket
den [Fyll i datum]

Förslag till Myndigheten för civilt försvars föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning;

beslutade den [Fyll i datum]

Myndigheten för civilt försvar föreskriver[1] följande med stöd av 38 § p. 5 och 39 § p. 1 cybersäkerhetsförordningen (2025:1507) och beslutar följande allmänna råd.

Allmänna råd har en annan juridisk status än föreskrifter. De är inte tvingande. Deras funktion är att förtydliga innebörden i lag, förordning och föreskrifter och att ge generella rekommendationer om deras tillämpning.

1 kap. Inledande bestämmelser

Tillämpningsområde

1 § Dessa föreskrifter och allmänna råd innehåller bestämmelser om säkerhetsåtgärder och utbildning som avses i 2 kap. 3 och 4 §§ cybersäkerhetslagen (2025:1506).

För verksamhetsutövare som uteslutande bedriver sektorsverksamhet inom digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster (mellan företag), post- och budtjänster samt rymden gäller endast kraven på ledningens utbildning i 2 kap. 1 § i denna författning.

2 § Om annan författning innehåller bestämmelser som ställer högre krav än kraven i dessa föreskrifter tillämpas den bestämmelsen.

[1] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148, i den ursprungliga lydelsen (NIS2-direktivet).

Ordförklaringar

3 § Uttryck i dessa föreskrifter och allmänna råd har samma betydelse som i cybersäkerhetslagen.

4 § I dessa föreskrifter och allmänna råd avses med

cybersäkerhetskris	en sådan storskalig cybersäkerhetsincident eller kris som en cyberkrishanterings-myndighet ansvarar för hanteringen av enligt artikel 9 i NIS2-direktivet,
digital miljö	den samlade mängden system som verksamhetsutövaren använder för att bedriva intern verksamhet och tillhandahålla externa tjänster. Består av produktionsmiljö och, i tillämpliga fall, utvecklings-, test- respektive utbildningsmiljö,
information i behov av utökat skydd	information som på grund av externa krav kräver en viss nivå av skydd avseende konfidentialitet, riktighet inklusive autenticitet, eller tillgänglighet alternativt information som verksamhetsutövaren vid värdering bedömer ha behov av motsvarande nivå av skydd,
it-segment	ett nätverkssegment som är inrättat för andra system än sådana system som placeras i ot-segment,
ot-segment	ett nätverkssegment som är inrättat för system som används för att styra, övervaka och inhämta information från cyberfysiska system,
produktionsmiljö	de system i den digitala miljön som används för att bedriva verksamhet förutom verksamhet som bedrivs i utvecklings- test- och utbildningsmiljö. Består av it-segment och ot-segment,
redundant funktion	två eller flera, identiska eller olika, funktioner som oberoende av varandra uppfyller samma syfte,

sektorskritiskt system	ett system som är nödvändigt för att kunna bedriva intern verksamhet eller tillhandahålla externa tjänster inom sektorsverksamhet,
sektorsverksamhet	sådan verksamhet som omfattas av cybersäkerhetslagen,
system	nätverks- och informationssystem enligt 1 kap. 2 § p. 16 cybersäkerhetslagen,
systematiskt och riskbaserat arbete med cybersäkerhet	arbete som bedrivs med stöd av interna regler och arbetssätt för att omhänderta risker när verksamhetsutövaren inriktar, upprättar, genomför, övervakar, kontrollerar, underhåller och utvecklar sin cybersäkerhet,
särskilda it- och ot-utrymmen	en lokal med tillträdesbegränsning eller ett låst skåp som är särskilt utformat för att skydda hårdvara i syfte att säkerställa systemens funktionalitet och behov av fysiskt skydd,
viktig samhällsfunktion	en samhällsfunktion som är nödvändig för samhällets grundläggande behov, värden eller säkerhet.

2 kap. Ledningens utbildning om säkerhetsåtgärder

1 § Ledningen ska ha den kunskap och kompetens som krävs för att fastställa mål och inriktning för verksamhetsutövarens cybersäkerhet, bedöma vilka säkerhetsåtgärder som verksamhetsutövaren behöver genomföra för att upprätthålla en lämplig nivå av cybersäkerhet utifrån identifierade risker och övervaka genomförandet av säkerhetsåtgärderna.

Allmänna råd

Ledningens utbildning bör omfatta

- ledningens roll i ett systematiskt och riskbaserat cybersäkerhetsarbete inklusive relevant terminologi och reglering,
- vilken betydelse cybersäkerheten hos verksamhetsutövaren har för att upprätthålla viktiga samhällsfunktioner,
- riskhantering och övervakning som ett stöd för att leda och styra arbetet med cybersäkerhet, samt
- för ledningen relevanta interna regler, arbetssätt och stöd.

3 kap. Organisatoriska säkerhetsåtgärder

Systematiskt och riskbaserat arbete med cybersäkerhet

1 § Verksamhetsutövaren ska bedriva ett systematiskt och riskbaserat cybersäkerhetsarbete utifrån ett allriskperspektiv. Arbetet ska integreras med befintligt sätt att leda och styra organisationen. I arbetet ska även ingå att

1. identifiera och analysera externa krav, interna behov och risker avseende cybersäkerhet,
2. utifrån externa krav, interna behov och risker utforma och genomföra säkerhetsåtgärder,
3. följa upp och utvärdera risker och säkerhetsåtgärder, samt
4. vid behov förbättra säkerhetsåtgärder.

2 § Verksamhetsutövaren ska identifiera och hantera behovet av att använda relevanta standarder i cybersäkerhetsarbetet.

Allmänna råd

Som stöd för arbetet bör följande eller motsvarande standarder användas

- Svensk standard SS-ISO/IEC 27001:2022 Informationssäkerhet – cybersäkerhet och integritetsskydd – Ledningssystem för informationssäkerhet – Krav, och
- Svensk standard SS-EN ISO/IEC 27002:2022 Informationssäkerhet – cybersäkerhet och integritetsskydd – Informationssäkerhetsåtgärder.

Interna regler och arbetssätt

3 § Verksamhetsutövaren ska fastställa de interna regler och arbetssätt som behövs för att vidta lämpliga och proportionella säkerhetsåtgärder utifrån externa krav, interna behov och identifierade risker avseende cybersäkerhet.

Interna regler och arbetssätt ska kommuniceras till berörd egen och inhyrd personal och uppdateras vid behov.

Verksamhetsutövaren ska identifiera och hantera behovet av att dokumentera och spara information som kan behövas vid uppföljning och utvärdering respektive tillsyn.

Allmänna Råd

Interna regler och arbetssätt bör utgå från ledningens mål och inriktning för cybersäkerheten samt vid behov kompletteras med stöd för hur interna regler och arbetssätt ska användas.
Av interna regler och arbetssätt bör följande framgå

- vilken säkerhetsåtgärd som avses,
- vilka roller som berörs,

- fastställandedatum samt vilken roll som ansvarar för att dokumentationen hålls uppdaterad,
- beskrivning av vad som ska göras, av vilken roll, hur och när,
- vilka beslut som ska fattas, av vilken roll och när, samt
- hur resultatet av efterlevnaden av interna regler och arbetssätt ska dokumenteras.

Verksamhetsutövaren bör, för att kunna bedöma ändamålsenlighet och effektivitet av cybersäkerheten vid uppföljning och utvärdering respektive tillsyn, spara interna regler och arbetssätt samt relevant dokumentation över hur de har tillämpats.

Bedömningen av vilken information som ska dokumenteras och hur länge dokumentationen ska sparas bör utgå från de behov som verksamhetsutövaren har avseende uppföljning och utvärdering samt de underlag som verksamhetsutövaren bedömer behövs vid tillsyn.

Roller, ansvarsområden och befogenheter

4 § För att verksamhetsutövaren ska kunna vidta lämpliga och proportionella säkerhetsåtgärder ska ledningen godkänna och övervaka genomförandet av säkerhetsåtgärder genom att säkerställa att

1. det finns fastställda mål och inriktning för cybersäkerheten,
2. ledningens uppgifter i arbetet med cybersäkerhet är tydliggjorda,
3. det finns resurser för att bedriva ett systematiskt och riskbaserat cybersäkerhetsarbete,
4. de roller och ansvarsområden som arbetet med cybersäkerhet kräver har tilldelats tillräckliga befogenheter och resurser, samt
5. ledningen, som en del av sin övervakning, vid behov men minst en gång per år blir informerad om genomförandet av säkerhetsåtgärderna och verksamhetsutövarens nivå på cybersäkerhet.

Allmänna råd

I ledningens uppgifter i arbetet med cybersäkerhet bör ingå att fastställa

- kriterier för riskacceptans,
- prioriteringsordning för återställning av verksamheter, och
- vilka system som är sektorskritiska.

Ledningen bör säkerställa att det finns ett utpekat ansvar och tillräckliga resurser för att kunna hålla sig inom acceptabla tider för otillgänglighet och nedsatt funktionalitet i sektorskritiska system under samhällsstörningar.

5 § För att kunna bedriva ett systematiskt och riskbaserat cybersäkerhetsarbete ska verksamhetsutövaren utse de roller och ansvarsområden som ett sådant arbete kräver och tilldela dessa de befogenheter som behövs för att kunna utföra tilldelade uppgifter.

Verksamhetsutövaren ska utse roller eller ansvarsområden för samordning av cybersäkerhetsarbetet (samordnare), för säkerheten i informations-

behandling i system (informationsägare) och för säkerheten i system (systemägare).

All informationsbehandling i system ska ha en utsedd informationsägare och alla system i verksamhetsutövarens digitala miljö ska ha en utsedd systemägare.

6 § Samordnaren eller motsvarande, ska ha befogenhet att samordna det systematiska och riskbaserade arbetet med cybersäkerhet och utvärdera nivån på cybersäkerheten i förhållande till externa krav, interna behov och identifierade risker. Samordnaren eller motsvarande ska säkerställa att de underlag som ledningen behöver för att kunna övervaka genomförandet av säkerhetsåtgärderna och bedöma verksamhetsutövarens nivå av cybersäkerhet sammanställs.

Allmänna råd

I sammanställningen av underlag till ledningen bör följande ingå

- uppgifter om hot och risker som bedöms som allvarliga för verksamhetsutövarens cybersäkerhet,
- uppgifter om bristande cybersäkerhet hos leverantörer och i digitala leveranskedjor,
- resultatet av intern och extern revision samt genomförd tillsyn avseende cybersäkerheten
- samordnarens utvärdering av verksamhetsutövarens nivå av cybersäkerhet, samt
- identifierade hinder för att uppnå ledningens mål och inriktning för cybersäkerheten och föreslagna åtgärder för att undanröja sådana hinder.

Samordnaren bör vid utvärderingen av verksamhetsutövarens nivå av cybersäkerhet utgå från följande underlag avseende cybersäkerheten

- ledningens mål och inriktning,
- informationsklassningar och riskanalyser samt aktuella åtgärdsplaner,
- uppföljningar och utvärderingar av införda säkerhetsåtgärder,
- information om inträffade incidenter och tillbud samt genomförda grundorsaksanalyser,
- utvärderingar av cybersäkerheten hos leverantörer och i digitala leveranskedjor, samt
- interna och externa revisioner samt genomförd tillsyn.

7 § Informationsägaren eller motsvarande, ska för den information som denne ansvarar för, ha befogenhet att säkerställa att den är värderad, att riskanalys genomförs vid behov och att informationen endast behandlas om lämpliga och proportionella säkerhetsåtgärder har införts.

Informationsägaren eller motsvarande ska informera berörd systemägare om identifierade krav på cybersäkerhet inklusive vad som är acceptabla tider för otillgänglighet och nedsatt funktionalitet för informationsbehandlingen.

8 § Systemägaren eller motsvarande, ska för system som denne ansvarar för, ha befogenhet att säkerställa att riskanalyser genomförs vid behov och att informationsägarens identifierade krav på cybersäkerhet avseende systemen uppfylls. Systemägaren eller motsvarande ansvarar också för att systemen, under hela deras livslängd, är skyddade med lämpliga och proportionella säkerhetsåtgärder.

Allmänna råd

Verksamhetsutövaren bör utse systemägare för utkontrakterad informationsbehandling för att kunna stödja informationsägaren avseende kravställning på och uppföljning av säkerhetsåtgärderna hos leverantören.

Personalsäkerhet

9 § För att förebygga att personal orsakar incidenter på grund av olämplighet eller okunskap ska verksamhetsutövaren fastställa

1. vilka kontroller som ska genomföras i samband med rekrytering av inhyrd och egen personal utifrån vilken information och vilka system de ska få tillgång till,
2. vilka kontroller som ska genomföras av egen och inhyrd personal vid förändrad åtkomst till information och system, samt
3. vilka utbildningar, övningar och andra informationsinsatser avseende cybersäkerhet som egen och inhyrd personal ska genomföra innan och under anställning eller uppdrag.

Allmänna råd

För att vid rekrytering av egen och inhyrd personal kunna bedöma deras lämplighet och kunskap om cybersäkerhet bör identitetskontroll, intervju, kontakt med referenser samt verifiering av akademiska, yrkesmässiga och övriga kvalifikationer genomföras.

Informationsinsatser avseende cybersäkerhet till egen och inhyrd personal bör inkludera

- grundläggande förståelse för varför cybersäkerhet behövs och hur cybersäkerhet uppnås,
- förståelse för relevanta interna regler och arbetssätt, samt
- vilket stöd som finns tillgängligt för att uppnå cybersäkerhet.

Utbildningar och övningar avseende cybersäkerhet för egen personal bör vara anpassade utifrån deras roller, ansvarsområden och befogenheter i arbetet med cybersäkerhet.

Verksamhetsutövaren bör upprätta en utbildningsplan där det framgår när och hur informationsinsatser, utbildningar och övningar ska genomföras samt när och hur uppföljning och utvärdering ska göras.

Verksamhetsutövaren bör informera egen och inhyrd personal som avslutar en anställning eller uppdrag om begränsningar i användandet av information som denne har fått tillgång till hos verksamhetsutövaren.

Omvärldsbevakning

10 § För att kunna hålla sig uppdaterad om hot, sårbarheter, teknisk utveckling, rättsliga krav och tillgängligt stöd av betydelse för verksamhetsutövarens cybersäkerhet, ska verksamhetsutövaren bedriva omvärldsbevakning. Verksamhetsutöveran ska inhämta relevant information från

1. leverantörer av hård- och mjukvara i den digitala miljön, och
2. det nationella cybersäkerhetscentret (NCSC), en del av Försvarets radioanstalt, och särskilt de däri ingående funktionerna nationell CSIRT-enhet och cyberkrishanteringsmyndighet.

Verksamhetsutövaren ska ansluta sig till automatiska notifieringar av tekniska sårbarheter (ANTS) hos den nationella CSIRT-enheten.

Verksamhetsutövaren ska identifiera och hantera behovet av att, om möjligt, ansluta sig till stöd för informationsutbyte om cyberhot (MISP-SE) hos den nationella CSIRT-enheten.

Allmänna råd

Verksamhetsutövaren bör även som en del av sin omvärldsbevakning inhämta relevant information från

- relevanta tillsynsmyndigheter,
- Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE) hos det nationella cybersäkerhetscentret (NCSC), och
- Europeiska unionens cybersäkerhetsbyrå (ENISA).

Informationsklassning

11 § För att identifiera vilka konsekvenser som bristande cybersäkerhet kan få för information som behandlas i system ska verksamhetsutövaren värdera informationen utifrån vilken nivå av skydd informationen behöver ha avseende konfidentialitet, riktighet inklusive autenticitet, och tillgänglighet.

Allmänna råd

Verksamhetsutövaren bör i sin informationsklassning utifrån verksamhetens behov fastställa

- vilka kriterier som ska användas vid bedömningen av konsekvenser, och
- antalet nivåer och tillhörande kriterier som ska användas vid informationsklassning.

Verksamhetsutövaren bör även säkerställa att nivåer och kriterier för informationsklassning är identiska med, eller kan relatera till, motsvarande nivåer och kriterier för konsekvensbedömning som används vid riskanalys.

Riskhantering

12 § För att kunna identifiera vilka lämpliga och proportionella säkerhetsåtgärder som ska genomföras i den digitala miljön ska verksamhetsutövaren identifiera, analysera och värdera risker utifrån deras konsekvens och sannolikhet. Verksamhetsutövaren ska utforma nivåer och tillhörande kriterier för bedömning av konsekvenser och sannolikhet så att risker kan jämföras över tid.

Risker ska värderas för

1. all informationsbehandling i system,
2. enskilda system och segment i produktionsmiljön, samt
3. den digitala miljön i sin helhet.

Verksamhetsutövaren ska värdera risker inför utkontraktering av informationsbehandling samt risker med avtal och överenskommelser om förvärv och utkontraktering som innehåller otillräckliga krav på cybersäkerhet. Verksamhetsutövaren ska även värdera risker för sina digitala leveranskedjor.

Den digitala miljöns arkitektur liksom resultatet av informationsklassning och omvärldsbevakning ska beaktas i arbetet med risker.

Allmänna råd

Verksamhetsutövaren bör omhänderta riskerna med aggregering och ackumulering av information. Vid förändrade hot och nya sårbarheter bör verksamhetsutövaren uppdatera genomförda riskanalyser.

Verksamhetsutövaren bör, utöver att värdera risker för sina digitala leveranskedjor kopplade till sina direkta leverantörer, även värdera risker som härrör från dennes eventuella underleverantörer. Vid en värdering av risker för de digitala leveranskedjorna bör verksamhetsutövaren beakta resultatet av de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor som utförs i enlighet med artikel 22.1 i NIS2-direktivet.

13 § För att kunna genomföra lämpliga och proportionella säkerhetsåtgärder ska verksamhetsutövaren vid valet av säkerhetsåtgärder utgå från resultatet av genomförda riskanalyser och fastställda kriterier för riskacceptans.

Valda säkerhetsåtgärder och de risker som dessa säkerhetsåtgärder omhändertar ska dokumenteras i en åtgärdsplan eller motsvarande. Av åtgärdsplanen ska det framgå vilken roll eller vilket ansvarsområde som ansvarar för att säkerhetsåtgärden genomförs och när den ska vara genomförd.

Allmänna råd

Åtgärdsplanen eller motsvarande bör innehålla en motivering för valet av respektive säkerhetsåtgärd och vilka andra säkerhetsåtgärder som har övervägts.

Verksamhetsutövaren bör värdera risken efter att säkerhetsåtgärden har genomförts.

Kontinuitetshantering

14 § För att kunna ha beredskap att bedriva verksamhet vid störningar i produktionsmiljön ska verksamhetsutövaren på förhand fastställa acceptabla tider för otillgänglighet och nedsatt funktionalitet för informationsbehandling och system.

Verksamhetsutövaren ska

1. fastställa om och när alternativa arbetssätt ska användas,
2. bedöma behovet av redundanta funktioner, samt
3. planera för och öva hur situationer med otillgänglighet och nedsatt funktionalitet i informationsbehandlingen och system ska hanteras.

Verksamhetsutövaren ska identifiera och hantera behovet av att fastställa acceptabla tider för otillgänglighet och nedsatt funktionalitet, bedöma behovet av redundanta funktioner samt planera för och öva hur situationer med otillgänglighet och nedsatt funktionalitet för utvecklings-, test-, och utbildningsmiljö ska hanteras.

Allmänna råd

Verksamhetsutövaren bör fastställa hur och när återgång till ordinarie arbetssätt ska göras efter det att alternativa arbetssätt har använts.

Återställning av sektorskritiska system bör övas vid behov men minst en gång per år.

Incidenthantering

15 § För att minimera konsekvenserna av incidenter och tillbud ska verksamhetsutövaren säkerställa att dessa kan upptäckas, analyseras och begränsas i omfattning.

Verksamhetsutövaren ska kunna återhämta sig från och lära sig av incidenter i den digitala miljön.

Allmänna råd

Verksamhetsutövaren bör säkerställa att det är enkelt för personal och mottagare av externa tjänster att anmäla incidenter och tillbud.

Verksamhetsutövaren bör inom incidenthanteringen uppfylla externa krav på rapportering av incidenter och informationsskyldighet till mottagare av externa tjänster som berörs av incidenten.

Verksamhetsutövaren bör säkerställa att risken för ytterligare incidenter eller tillbud beaktas vid valet av åtgärder som ska begränsa omfattning och konsekvenser av en incident.

Verksamhetsutövaren bör ha kontakt med berörda leverantörer vid incidenter och utreda incidentens grundorsak om den inte redan är känd.

Krishantering

16 § För att kunna minimera konsekvenser av incidenter som inte kan omhändertas inom incidenthanteringen ska verksamhetsutövaren fastställa hur roller, ansvarsområden och befogenheter fördelas under en kris samt hur kriskommunikation ska genomföras.

Verksamhetsutövaren ska identifiera och hantera behovet av tillgång till system för intern och extern kriskommunikation med höga krav på robusthet och tillgänglighet för informationsdelning och samverkan under kriser.

Allmänna råd

Vid krishantering bör etablerad stabsmetodik och struktur användas. Verksamhetsutövaren bör öva sin krishantering vid behov men minst en gång per år.

För att stärka förmågan till kriskommunikation mellan olika organisationer som kan komma att påverkas vid kriser bör verksamhetsutövaren öva användandet av det webbaserade informationsdelningssystemet WIS som tillhandahålls av Myndigheten för civilt försvar.

Uppföljning och utvärdering

17 § För att kunna bedöma effektiviteten av genomförda säkerhetsåtgärder ska verksamhetsutövaren följa upp och utvärdera om säkerhetsåtgärderna är lämpliga och proportionella i förhållande till externa krav, interna behov och identifierade risker. Uppföljning och utvärdering ska ske vid behov men minst en gång per år.

Allmänna råd

Verksamhetsutövaren bör använda etablerade metoder för uppföljning och utvärdering av säkerhetsåtgärderna såsom granskning, mätning och tester. Dessa kan ske i form av egenkontroll. intern eller extern revision.

Verksamhetsutövaren bör säkerställa att uppföljning och utvärdering genomförs i samband med

- att säkerhetsåtgärder införs eller förändras,

- att förändrade hot eller när nya sårbarheter identifieras,
- grundorsaksanalys efter betydande incidenter, samt
- verksamhetsuppföljning, omorganisation, förändrade rättsliga krav och inför utkontraktering.

Uppföljning och utvärdering av det systematiska och riskbaserade arbetet med cybersäkerhet bör även omfatta hur ledningens mål och inriktning efterlevs och om interna regler, arbetssätt och stöd motsvarar verksamhetens behov. Vid uppföljning och utvärdering bör även brister och oklarheter avseende tilldelade befogenheter, resurser och arbetsuppgifter samt bristande kompetensförsörjning bedömas.

---

4 kap. Tekniska och driftrelaterade säkerhetsåtgärder

Förvärv av system och utkontraktering av informationsbehandling

1 § För att säkerställa att verksamhet kan bedrivas med en tillräcklig nivå av cybersäkerhet ska verksamhetsutövaren, innan förvärv av system eller inför utkontraktering av informationsbehandling, utvärdera potentiella leverantörer.

Verksamhetsutövaren ska säkerställa att de krav som ställs på verksamhetsutövaren i denna författning uppfylls av leverantören utom i de delar kravet i sin helhet uppfylls av verksamhetsutövaren.

Innan ett avtal eller en överenskommelse tecknas om förvärv av system eller utkontraktering av informationsbehandling ska verksamhetsutövaren ha bedömt att leverantören kommer att kunna uppfylla ställda krav på cybersäkerhet under hela avtalstiden.

Verksamhetsutövaren ska identifiera och hantera behovet av att komplettera avtal och överenskommelser som har ingåtts före den 1 oktober 2026 med krav på cybersäkerhet.

2 § Verksamhetsutövaren ska identifiera och hantera behovet av att välja system och tjänster som är certifierade i enlighet med europeiska ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster enligt artikel 1 st. 1 p. b i EU:s cybersäkerhetsförordning.[2]

[2] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten). I denna författning benämd EU:s cybersäkerhets-förordning.

Allmänna råd

Sektorskritiska system bör vara certifierade i enlighet med europeiska ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster enligt artikel 1 st. 1 p. b i EU:s cybersäkerhetsförordning.

3 § Innan förvärv av system och inför utkontraktering av informationsbehandling ska verksamhetsutövaren säkerställa att lämpliga och proportionella säkerhetsåtgärder kan genomföras och förvaltas över tid.

Allmänna råd

Innan avtal och överenskommelser tecknas om utkontraktering av informationsbehandling bör verksamhetsutövaren säkerställa att informationsklassning är genomförd för den information som ska utkontrakteras och riskerna med utkontrakteringen är omhändertagna. Verksamhetsutövaren bör säkerställa att krav på säkerhetsåtgärder som behöver ställas på leverantören relaterade till informationsbehandlingen är identifierade.

Avtal eller överenskommelse om utkontraktering av informationsbehandling bör reglera vilka säkerhetsåtgärder leverantören ska vidta och

- att leverantören utser en systemägare och vilket ansvar denne har gentemot verksamhetsutövaren,
- vilken kompetens avseende cybersäkerhet leverantören behöver ha,
- när och hur leverantören ska informera verksamhetsutövaren, om misstänkta och inträffade incidenter och tillbud, om identifierade hot och sårbarheter samt om förändringar i system som kan påverka avtalsefterlevnaden,
- hur risker i verksamhetsutövarens digitala leveranskedjor som härrör från leverantörens underleverantörer ska omhändertas och delges verksamhetsutövaren,
- i vilken omfattning leverantören ska öva incident-, kontinuitets- och krishantering med verksamhetsutövaren, samt
- hur leverantören ska följa upp sin egen och eventuella underleverantörers efterlevnad av ställda krav på säkerhetsåtgärder i avtal och överenskommelser samt ,
- hur verksamhetsutövaren ska följa upp leverantörens efterlevnad av ställda krav.

Innan utkontrakterad informationsbehandling inleds bör verksamhetsutövaren kontrollera att riskerna med utkontrakteringen är omhändertagna**,** informationsägare är utsedda för den informationshantering som utkontrakteras, och tilltänkt leverantör uppfyller ställda krav på säkerhetsåtgärder.

Utveckling, underhåll och avveckling av system

4 § För att kunna motverka att sårbarheter uppstår vid utveckling och underhåll av den digitala miljön ska verksamhetsutövaren inför och under utvecklingen samt vid underhåll av system säkerställa att

1. informationsägare och systemägare involveras i arbetet för att kunna identifiera och hantera behov av säkerhetsåtgärder,
2. informationsklassning har genomförts och hålls uppdaterad,
3. riskanalys är genomförd och hålls uppdaterad,
4. åtgärdsplanen hålls uppdaterad, och
5. etablerade metoder för säker utveckling följs.

5 § Innan beslut fattas om att för första gången driftsätta ett system i den digitala miljön ska verksamhetsutövaren säkerställa att

1. det finns nödvändig dokumentation för drift och förvaltning,
2. granskningar och säkerhetstester har genomförts för att säkerställa att valda säkerhetsåtgärder är lämpliga och proportionella,
3. tilldelade resurser för drift och underhåll av systemet är tillräckliga,
4. identifierade krav på säkerhetsåtgärder för systemet är genomförda, och
5. beslut om att påbörja informationsbehandlingen har fattats.

Om utveckling och underhåll av redan driftsatt system kan påverka säkerheten i den digitala miljön ska verksamhetsutövaren säkerställa att p. 1-5 omhändertas.

Framkommer brister avseende p. 1-5 ska dessa dokumenteras och eventuella risker med bristerna omhändertas.

6 § För att upprätthålla skyddet för information under en avveckling av system ska verksamhetsutövaren innan avvecklingen påbörjas säkerställa att

1. tilldelade resurser för avveckling av systemet är tillräckliga,
2. beslut om att avveckla informationsbehandlingen har fattats,
3. risker med avvecklingen har omhändertagits, och
4. åtgärdsplan för avvecklingen finns.

Driftrelaterad dokumentation

7 § För att kunna upprätthålla den driftsäkerhet som verksamhetsutövaren behöver ska verksamhetsutövaren hålla dokumentation över arkitekturen för den digitala miljön uppdaterad.

Allmänna råd

Av dokumentationen över den digitala miljön bör framgå

- vilka miljöer den är indelad i, det vill säga produktions-, utvecklings-, test- och utbildningsmiljö,

- vad respektive miljö innehåller avseende segment, system, hårdvara, och mjukvara,
- vilka informationsflöden som finns mellan olika interna miljöer, mellan system, samt till och från den digitala miljön, och
- vilken verksamhet, om någon, som bedrivs med stöd av utkontrakterad informationsbehandling.

Tekniskt systemstöd bör användas för att hålla dokumentationen uppdaterad. Arkitekturen bör visualiseras i en systemkarta.

---

8 § För att verksamhetsutövaren skyndsamt ska kunna omhänderta sårbarheter och incidenter i den digitala miljön och bedöma konsekvenserna av dessa ska verksamhetsutövaren hålla en uppdaterad förteckning över relevant information om den digitala miljön.

Allmänna råd

Förteckningen över den digitala miljön bör innehålla information om

- vilka system som ingår i produktionsmiljön samt kontaktuppgifter till berörda systemägare och informationsägare,
- kontaktuppgifter till leverantörer av hård- och mjukvara som används i produktionsmiljön,
- vilka system som är sektorskritiska och vilka som används för att tillhandahålla verksamhetsutövarens externa tjänster, samt
- vilka, om några, system i utvecklings-, test- eller utbildningsmiljö som bedöms vara kritiska för att skyndsamt kunna omhänderta sårbarheter och incidenter i produktionsmiljön.

Verksamhetsutövaren bör dokumentera vilken informationsbehandling som är utkontrakterad samt kontaktuppgifter till leverantören och till verksamhetsutövarens berörda informationsägare. Förteckningen bör även innehålla kontaktuppgifter till sådana funktioner hos leverantörer som ger stöd vid sårbarheter och incidenter.

---

9 § För att kunna upprätthålla säker drift och möjliggöra återställning av system i produktionsmiljön ska verksamhetsutövaren hålla drift-dokumentationen för systemen uppdaterad.

Verksamhetsutövaren ska identifiera och hantera behovet av att hålla driftdokumentation för system i utvecklings-, test- och utbildningsmiljö uppdaterad.

Allmänna råd

Av driftdokumentationen för ett system bör framgå

- vilken verksamhet och vilken informationsbehandling som systemet stödjer samt om systemet används för sektorskritisk verksamhet,
- om och varför systemet är nödvändigt för att upprätthålla viktiga samhällsfunktioner hos andra organisationer,

- om information i behov av utökat skydd behandlas i systemet,
- referens till aktuell riskanalys och risker som inte kunnat omhändertas på ett tillfredställande sätt,
- vilka behov av cybersäkerhet som systemet behöver uppfylla och vilka säkerhetsåtgärder som har genomförts för att möta identifierat behov av cybersäkerhet,
- acceptabla tider för otillgänglighet och nedsatt funktionalitet och hur systemet återställs,
- om systemet är placerat i it-segment eller ot-segment,
- vilken hårdvara som används och dess version och vilken mac-adress, ip-adress eller identifierare som används för hårdvara,
- vilken mjukvara som används och dess version,
- hur hård- och mjukvara är konfigurerad,
- resurser som behövs för drift och underhåll av systemet,
- kontaktuppgifter till berörd systemägare och till berörda informationsägare, samt
- referens till relevanta användarmanualer för systemet.

Segmentering

10 § För att minimera konsekvenser och förhindra spridning av incidenter orsakade av angrepp mot och misstag i produktionsmiljön ska verksamhetsutövaren dela in miljön i segment. Verksamhetsutövaren ska placera följande system i produktionsmiljöns it-segment i separata segment:

1. System som används för gästnätverk.
2. System i den interna digitala miljön som sammankopplas med system hos leverantör.
3. System som tillhandahåller externa tjänster.
4. System som innehåller sårbarheter som inte kan omhändertas på ett tillfredställande sätt.

Verksamhetsutövaren ska identifiera och hantera behovet av ot-segment och av att placera enskilda system, ett begränsat antal system eller system med liknande funktion, användning eller skyddsbehov i separata segment i den digitala miljön.

Allmänna råd

Verksamhetsutövaren bör införa segment i produktionsmiljön för

- klienter för användare och för systemadministration,
- sektorskritiska system,
- centrala säkerhetsfunktioner i form av behörighetshantering säkerhetsloggning, säkerhetskopiering, övervakning av system, filtrering av extern kommunikation och liknade,
- centrala stödfunktioner i form av skrivare, skanner och liknande funktioner, samt
- trådlösa nätverk för personal.

11 § Verksamhetsutövarens ska bedriva utveckling, test och utbildning som kan påverka säkerheten i produktionsmiljöns it-segment i en från produktionsmiljön avskild utvecklings-, test- respektive utbildningsmiljö.

Verksamhetsutövaren ska identifiera och hantera behovet av att bedriva utveckling, test och utbildning som kan påverka säkerheten i produktionsmiljöns ot-segment i en från produktionsmiljön avskild utvecklings-, test- respektive utbildningsmiljö.

Behörighetshantering och autentisering

12 § För att endast behöriga användare och system ska få åtkomst till olika delar av den digitala miljön ska verksamhetsutövaren genom behörighetshantering fastställa hur digitala identiteter, behörigheter och autentiseringsuppgifter utformas, tilldelas, används, förändras, avslutas och skyddas.

Allmänna råd

Verksamhetsutövaren bör

- tidsbegränsa tilldelade digitala identiteter och behörigheter,
- säkerställa att autentiseringsuppgifter har tillräcklig längd och komplexitet för att försvåra angrepp,
- använda tekniska system som stöd för hantering och kontroll av digitala identiteter, behörigheter och autentiseringsuppgifter, samt
- identifiera vilka externa tjänster som ska vara åtkomliga utan kontroll av digitala identiteter eller behörigheter.

13 § Verksamhetsutövaren ska låsa en digital identitet efter ett fastställt antal misslyckade inloggningsförsök och låsa, blockera eller ta bort digitala identiteter för användare eller system som inte längre ska ha åtkomst till system eller den digitala miljön.

14 § Verksamhetsutövaren ska inte tilldela användare och system behörighet till mer information eller fler system än vad som är nödvändigt för att bedriva verksamheten och upprätthålla cybersäkerheten.

Systemadministrativ behörighet ska tilldelas restriktivt och endast användas för systemadministration.

Verksamhetsutövaren ska inte tillåta att autentiseringsuppgifter som används i produktionsmiljön också används i utvecklings-, test- och utbildningsmiljö.

Allmänna råd

Verksamhetsutövaren bör

- genomföra åtkomstkontroll till information i centrala stödfunktioner i form av skrivare, skanner och liknande utrustning innan åtkomst beviljas,
- administrera olika segment av produktionsmiljön med olika systemadministrativa behörigheter, samt
- begränsa omfattning och tid för systemadministrativa behörigheter som ges till leverantörer till aktuellt uppdrag.

15 § Verksamhetsutövaren ska använda flerfaktorsautentisering för åtkomst till system i it-segment som behandlar information som har behov av utökat skydd. Flerfaktorsautentisering ska även användas för personals och leverantörs åtkomst till den digitala miljön via externt nätverk och för systemadministrativ åtkomst till system i produktionsmiljön.

Verksamhetsutövaren ska identifiera och hantera behov av flerfaktorsautentisering vid annan åtkomst till information och system i den digitala miljön.

16 § Verksamhetsutövaren ska identifiera och hantera behovet av att mottagare av externa tjänster identifierar sig med e-legitimation eller motsvarande för åtkomst till dessa.

17 § Verksamhetsutövaren ska identifiera och hantera behovet av att andra organisationer och enskilda personer kan verifiera verksamhetsutövarens identitet vid kontakt via digitala kanaler.

Allmänna råd

Verksamhetsutövaren bör säkerställa att andra organisationer och enskilda personer kan verifiera verksamhetsutövarens identitet vid via e-post, sms, telefonsamtal och webbsidor. Verksamhetsutövaren bör tillhandahålla lättillgänglig information om hur sådan verifiering kan göras.

Övervakning, säkerhetsloggning och logganalys

18 § För att kunna upptäcka tekniska fel, intrång och andra brister i cybersäkerheten ska verksamhetsutövaren övervaka system och informationsflöden samt möjliggöra utredning av fel, intrång och andra brister i cybersäkerheten genom säkerhetsloggning. Säkerhetsloggarna ska skyddas mot obehörig åtkomst och sparas så länge de behövs för att kunna genomföra sådan utredning.

Verksamhetsutövaren ska identifiera och hantera behovet av realtidsövervakning i produktionsmiljön.

Allmänna råd

För att möjliggöra utredning av fel, intrång och andra brister i cybersäkerheten bör verksamhetsutövaren säkerställa att säkerhetsloggar innehåller tillräcklig information om vilken händelse som har inträffat, vilken användare och vilket system som har initierat händelsen, vilken information och vilka system som har påverkats samt vid vilken tidpunkt som händelsen inträffade.

Verksamhetsutövaren bör använda realtidsövervakning i produktionsmiljön för att skyndsamt upptäcka och agera på incidenter och tillbud i centrala säkerhetsfunktioner och sektorskritiska system.

19 § Verksamhetsutövaren ska, om det inte är uppenbart obehövligt, säkerhetslogga följande i den digitala miljön:

1. Obehörig åtkomst och försök till obehörig åtkomst.
2. Användning av systemadministrativ behörighet.
3. Förändring av konfigurationer i centrala säkerhetsfunktioner och sektorskritiska system.
4. Förändring av behörighet för användare och system.
5. Åtkomst till information i behov av utökat skydd.
6. Händelser som upptäckts genom övervakning och indikerar brister i cybersäkerheten.

Allmänna råd

Verksamhetsutövaren bör säkerhetslogga åtkomst till produktionsmiljön och till system som förutsätter en tilldelad behörighet.

20 § Verksamhetsutövaren ska analysera säkerhetsloggarna för att upptäcka och utreda fel, obehörig åtkomst och andra brister i cybersäkerheten.

Verksamhetsutövaren ska analysera säkerhetsloggar för varje system med ett intervall som är lämpligt utifrån externa krav, interna behov och identifierade risker.

Allmänna råd

Verksamhetsutövaren bör använda ett centralt systemstöd för att samla in, lagra och analysera säkerhetsloggarna.

Robust och korrekt tid

21 § För att kunna jämföra säkerhetsloggar vid incidenter som involverar andra organisationer ska verksamhetsutövaren använda robust och korrekt tid som är översättningsbar till den svenska tillämpningen av koordinerad universell tid, UTC (SP), i produktionsmiljön.

Verksamhetsutövaren ska identifiera och hantera behovet av att använda robust och korrekt tid som är översättningsbar till den svenska tillämpningen av koordinerad universell tid, UTC (SP) i utvecklings-, test- och utbildningsmiljön.

Allmänna råd

Verksamhetsutövaren bör använda tidstjänsten Swedish Distributed Time Service för robust och korrekt tid koordninerad till UTC (SP).

Skydd mot skadlig kod

22 § För att skydda system i it-segment mot angrepp med skadlig kod ska verksamhetsutövaren, om sådan mjukvara finns tillgänglig, använda mjukvara som ger tillräckligt skydd.

Allmänna råd

Verksamhetsutövaren bör skydda system i ot-segment mot angrepp med skadlig kod genom att, om sådan mjukvara finns tillgänglig, använda mjukvara som ger tillräckligt skydd.

Kryptering

23 § För att skydda information i system mot obehörig åtkomst och obehörig förändring vid överföring mellan och lagring i system ska verksamhetsutövaren identifiera och hantera behovet av att kryptera informationen i den digitala miljön.

Allmänna råd

Verksamhetsutövaren bör fastställa kriterier för val och godkännande av krypteringsalgoritmer, krypteringsprotokoll och nyckellängder samt fastställa när och hur krypteringsnycklar genereras, distribueras, används, återkallas, skyddas och förstörs.

24 § Verksamhetsutövaren ska använda kryptering för att skydda säkerhetsloggar och autentiseringsuppgifter vid överföring i den digitala miljön. Säkerhetsloggar, autentiseringsuppgifter och annan information i behov av utökat skydd ska skyddas med kryptering vid överföring till system utanför den digitala miljön.

Allmänna råd

Verksamhetsutövaren bör skydda säkerhetsloggar, autentiseringsuppgifter och information i behov av utökat skydd med kryptering vid lagring i den digitala miljön.

25 § För att försvåra angrepp genom manipulation av översättningen mellan domännamn och ip-adresser i domännamnssystemet (DNS) ska verksamhetsutövaren, om inte uppenbart obehövligt, använda Domain Name System Security Extensions (DNSSEC) för domännamn som verksamhetsutövaren registrerat i DNS.

Säkerhetskonfigurering

26 § För att försvåra angrepp mot system ska de konfigureras så att obehörig åtkomst försvåras och cybersäkerheten upprätthålls. Verksamhetsutövaren ska:

1. Byta ut förinställda autentiseringsuppgifter och ta bort, stänga av eller blockera funktioner i system som inte behövs.
2. Endast tillåta godkända informationsflöden till, från och inom den digitala miljön.
3. Identifiera och hantera behovet av att endast tillåta installation och användning av på förhand godkänd mjukvara.

Allmänna råd

Verksamhetsutövaren bör inte tillåta direktkommunikation mellan klienter och bör säkerställa att inaktiva sessioner automatiskt avslutas efter en fördefinierad tidsperiod.

Vid säkerhetskonfigurering bör leverantörens rekommendationer och relevanta standarder användas och säkerhetsfunktioner bör konfigureras så att säkerhet upprätthålls när tekniska fel och brister inträffar.

Verksamhetsutövaren bör använda tekniskt systemstöd för att följa upp att systemen är korrekt konfigurerade.

Säkerhetstester

27 § För att identifiera bristande cybersäkerhet i system, segment och den digitala miljön ska verksamhetsutövaren genom säkerhetstester säkerställa att valda tekniska säkerhetsåtgärder har införts och möter identifierade behov av säkerhet. Säkerhetstester ska användas för att kontrollera att

1. systemen är uppdaterade till senaste version,
2. publicerade sårbarheter är omhändertagna, och
3. valda konfigurationer har införts.

Allmänna råd

Verksamhetsutövaren bör säkerställa att etablerad testmetodik används för både automatiserade och manuella säkerhetstester.

Om sårbarheter som inte tidigare har publicerats upptäcks bör dessa rapporteras till den nationella CSIRT-enheten.

Återställning av förlorad information och säkerhetskopiering

28 § För att minska konsekvenserna för verksamheten om informationen i system har förlorats, förvanskats eller på annat sätt blivit otillgänglig, ska verksamhetsutövaren säkerställa att informationen kan återställas inom fastställda acceptabla tider för nedsatt funktionalitet och otillgänglighet.

Verksamhetsutövaren ska identifiera och hantera behovet av att säkerhetskopiera informationen.

Allmänna råd

För säkerhetskopiering bör det fastställas

- vilken information som ska säkerhetskopieras avseende programvara, konfiguration respektive behandlad information,
- hur ofta och på vilket sätt säkerhetskopior ska tas och hur kontroll ska göras av att informationen på säkerhetskopiorna är korrekt och komplett,
- hur säkerhetskopior ska skyddas mot obehörig åtkomst, obehörig förändring och fysisk skada och var och hur länge säkerhetskopiorna ska sparas, samt,
- hur återläsning av säkerhetskopior ska genomföras, och hur kontroll ska göras av att informationen som återlästs är korrekt och komplett

Minst en säkerhetskopia bör skyddas mot skadlig kod genom att lagras på hårdvara separerad från det system som informationen hämtats ifrån.

Intrångsdetektering och intrångsskydd

29 § För att kunna upptäcka och hindra angrepp mot den digitala miljön ska verksamhetsutövaren använda intrångsdetektering och intrångsskydd i produktionsmiljön.

Verksamhetsutövaren ska identifiera och hantera behovet av intrångsdetektering och intrångsskydd i utvecklings-, test- och utbildningsmiljön.

Ändringshantering

30 § För att minska risken för incidenter och tillbud som kan uppkomma vid ändringar i produktionsmiljön ska verksamhetsutövaren bedriva ändringshantering på ett strukturerat och spårbart sätt vid införande, uppgradering, uppdatering och avveckling av hård- och mjukvara i produktionsmiljön.

Verksamhetsutövaren ska identifiera och hantera behovet av att bedriva ändringshantering på ett strukturerat och spårbart sätt i utvecklings-, test- och utbildningsmiljö.

Allmänna råd

Verksamhetsutövaren bör genom ändringshantering säkerställa att endast godkända ändringar genomförs.
Mjukvara bör uppdateras till senaste version utan onödigt dröjsmål.

Verksamhetsutövaren bör fastställa vilka åtgärder som ska vidtas när en uppdatering eller uppgradering inte kan genomföras eller när pågående ändring behöver avbrytas.

31 § För att skydda system i it-segment mot kända sårbarheter ska verksamhetsutövaren genomföra säkerhetsuppdateringar skyndsamt.

Mjukvara som leverantören inte längre tillhandahåller säkerhetsuppdateringar för ska bytas ut eller uppgraderas utan onödigt dröjsmål.

Verksamhetsutövaren ska identifiera och hantera behovet av säkerhetsuppdateringar, uppdateringar och uppgraderingar i ot-segment.

Allmänna råd

Verksamhetsutövaren bör påbörja arbetet med att införa en säkerhetsuppdatering inom 72 timmar efter det att programvara som ger skydd mot sårbarheten har tillgängliggjorts.

5 kap. Fysiska säkerhetsåtgärder

Lokaler

1 § För att undvika obehörig fysisk åtkomst till, förlust av och fysisk skada på system ska verksamhetsutövaren skydda lokaler där information behandlas i system mot obehörigt tillträde genom tillträdesbegränsning och övervakning. Verksamhetsutövaren ska kontrollera personals och besökares identitet innan de ges tillträde till sådana lokaler förutom till utpekade besöksutrymmen.

Verksamhetsutövaren ska identifiera och hantera behovet av att inrätta särskilda it- och ot-utrymmen.

Allmänna råd

Verksamhetsutövaren bör säkerställa att det finns anpassat skalskydd för verksamheten.

Verksamhetsutövaren bör behandla information i behov av utökat skydd i sektioner skilda ifrån övriga lokaler och tilldela tillträde till särskilda it- och ot-utrymmen restriktivt och registreras tillträdet på individnivå.

Verksamhetsutövaren bör placera servrar och nätverksutrustning i särskilda it- och ot-utrymmen.

2 § Verksamhetsutövaren ska säkerställa, om det inte är uppenbart obehövligt, att särskilda it- och ot-utrymmen förses med övervakning och larm samt att åtgärder vidtas vid larm om obehörigt tillträde.

Allmänna råd

Verksamhetsutövaren bör säkerställa att övriga lokaler där information behandlas i system finns förses med övervakning och larm samt att åtgärder vitas vid larm om obehörigt tillträde.

3 § För att undvika förlust av, skada på eller funktionsstörning i system ska verksamhetsutövaren identifiera och hantera behovet av att skydda lokaler mot

1. brand,
2. vattenskador,
3. oacceptabel nivå av luftfuktighet, och
4. oacceptabel temperatur.

Tekniska försörjningssystem

4 § För att undvika skada på eller störning i system på grund av fel eller avbrott i tekniska försörjningssystem ska verksamhetsutövaren säkerställa tillräcklig funktionalitet i den digitala miljön avseende elförsörjning, elektroniska kommunikationsnät och elektroniska kommunikationstjänster, samt kyla,värme, och ventilation.

Verksamhetsutövaren ska identifiera och hantera behovet av att övervaka de tekniska försörjningssystemens funktion och säkerställa att larm genereras och åtgärder vidtas vid otillräcklig funktionalitet.

Verksamhetsutövaren ska identifiera och hantera behovet av redundanta funktioner för tekniska försörjningssystem.

6 kap. Sektorsspecifika säkerhetsåtgärder

Offentlig förvaltning

System för kriskommunikation

1 § För att kunna kommunicera med andra organisationer vid kriser ska verksamhetsutövare säkerställa cybersäkerheten i system som ska användas för intern och extern kriskommunikation vid kriser kontrolleras.

Allmänna råd

Verksamhetsutövaren bör kontrollera att kriskommunikationssystem kan användas på avsett sätt var tredje månad.

2 § Verksamhetsutövare ska identifiera och hantera behovet av att, om möjligt, använda Rakel (Radiokommunikation för effektiv ledning) eller SWEN (The Swedish Emergency Network) och SGSI (Swedish Government Secure Intranet) för kriskommunikation.

7 kap. Undantag

1 § Den myndighet som har mandat att utfärda föreskrifter enligt 38 § p. 5 och 39 § p. 1 cybersäkerhetsförordningen får i enskilda fall, och om det finns särskilda skäl, medge undantag från tillämpningen av dessa föreskrifter.

Denna författning träder i kraft [Klicka och skriv tidsangivelse].

Myndigheten för civilt försvar