Myndigheten för samhällsskydd och beredskaps författningssamling

Utgivare: Anna Asp, Myndigheten för samhällsskydd och beredskap
ISSN 2000-1886

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

Förslag till Myndighetens för samhällsskydd och beredskaps föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning;

beslutade den [Fyll i datum]

Myndigheten för samhällsskydd och beredskap föreskriver[1] följande med stöd av XX § förordningen (2025:XXX) om cybersäkerhet 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 §§ lagen (2025:XX) om cybersäkerhet.

För sektorsverksamhet inom digital infrastruktur, digitala leverantörer, informations- och kommunikationstjänster mellan företag (IKT-tjänster), post- och budtjänster och rymden gäller endast kraven på ledningens utbildning i 2 kap. 9 §.

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

Ordförklaring

3 § Termer och uttryck i dessa föreskrifter och allmänna råd har samma betydelse som i lagen (2025:XXX) om cybersäkerhet.

[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 (NIS2-direktivet).

I dessa föreskrifter och allmänna råd avses med

cybersäkerhetskris	storskalig cybersäkerhetsincident eller kris enligt artikel 9 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 (NIS2-direktivet),
digital miljö	den samlade mängden system som verksamhetsutövaren ansvarar för. Digital miljö delas in i produktionsmiljö och utvecklings-, test- och utbildningsmiljö,
it-segment	ett nätverkssegment som verksamhetsutövaren har inrättat för andra system än sådana som placeras i ot-segment. Är ett segment i produktionsmiljö och utvecklings-, test- och utbildningsmiljö,
ot-segment	ett nätverkssegment i en del av den digital miljön som verksamhetsutövaren har inrättat för system som används för att styra och övervaka cyberfysiska system, Är ett segment i produktionsmiljö och utvecklings-, test- och utbildningsmiljö,
produktionsmiljö	den av den digitala miljön som verksamhetsutövaren använder för sin produktion eller utförande av sitt uppdrag,
redundant funktion	två eller flera, identiska eller olika, funktioner som oberoende av varandra uppfyller samma syfte,
sektorskritiskt system	system som är nödvändigt för verksamhetsutövarens möjlighet att bedriva sektorsverksamhet,

sektorverksamhet	verksamhet som anges i bilaga 1 eller 2 till NIS2-direktivet. Med sektorverksamhet i offentlig förvaltning avses sådan verksamhet som en kommun, region eller statlig myndighet är skyldig att utföra enligt författning,
system	nätverks- och informationssystem enligt 1 kap. 2 § p 19 i cybersäkerhetslag (2025:XX),
systematiskt och riskbaserat arbete	arbete som bedrivs med stöd av interna regler och arbetssätt för att upprätta, genomföra, driva, övervaka, kontrollera, underhålla och utveckla organisationens cybersäkerhet utifrån risk,
säkerhetslogg	registrering av säkerhetsrelaterade händelser,
säkerhetskonfiguration	konfigurationer som påverkar cybersäkerheten,
särskilda it-utrymmen	en lokal eller ett låst skåp som är särskilt utformat för att skydda hårdvara i syfte att säkerställa systemens funktion och behov av fysiskt skydd,
viktig samhällfunktion	en viktig samhällsfunktion är en sådan samhällsfunktion som är nödvändig för samhällets grundläggande behov, värden eller säkerhet.

.

2 kap. Organisatoriska säkerhetsåtgärder

Systematiskt och riskbaserat arbete

1 § Verksamhetsutövarens arbete med cybersäkerhet ska vara systematiskt, riskbaserat och integrerat med befintliga sätt att leda och styra organisationen. Verksamhetsutövaren ska identifiera och hantera behovet av att använda relevanta standarder i arbetet.

Allmänna råd

Som stöd för arbetet bör följande eller motsvarande standarder användas:

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

---

2 § Det systematiska och riskbaserade arbetet ska minst omfatta att

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

Interna regler och arbetssätt

3 § Verksamhetsutövaren ska upprätta de interna regler och arbetssätt som behövs för arbetet med att genomföra lämpliga och proportionella säkerhetsåtgärder utifrån ett allriskperspektiv. Interna regler och arbetssätt ska dokumenteras och hållas uppdaterade. De ska

1. utgå från ledningens mål och inriktning,
2. utformas utifrån externa krav, interna behov och risker,
3. vid behov kompletteras med stöd för hur interna regler och arbetssätt ska tillämpas, samt
4. kommuniceras till berörd egen och inhyrd personal.

4 § Interna regler och arbetssätt ska minst innehålla

1. vilken säkerhetsåtgärd som avses,
2. vilken målgruppen är,
3. beslutsdatum samt vilken roll som ansvarar för att dokumentet hålls uppdaterat,
4. hur och när de interna regler och arbetssätt ska följas upp och utvärderas,
5. beskrivning av
   a) vad som ska göras,
   b) när det ska göras,
   c) hur det ska göras,
   d) vilka roller som ska göra vad,
   e) vilka beslut som ska fattas, när och av vilken roll, samt
6. hur resultatet av tillämpningen av interna regler och arbetssätt ska dokumenteras och när det ska följas upp och utvärderas.

Dokumentation av interna regler och arbetssätt ska bevaras i minst 5 år.

Dokumentation av resultatet av tillämpningen av interna regler och arbetssätt ska, om inte särskilda hinder identifierats, bevaras i minst 5 år.

Underlag enligt 2 kap. 24 § och de beslut som ledningen fattar med anledning av arbetet med övervakning av genomförandet av säkerhetsåtgärder ska bevaras i minst 5 år.

5 § I interna regler och arbetssätt ska minst följande ingå

1. organisatoriska säkerhetsåtgärder i enlighet med kapitel 2,
2. tekniska och driftrelaterade säkerhetsåtgärder i enlighet med kapitel 3,
3. fysiska säkerhetsåtgärder i enlighet med kapitel 4, och
4. relevanta sektorsspecifika säkerhetsåtgärder i enlighet med kapitel 5.

Ledningens ansvar för säkerhetsåtgärder

6 § Ledningens ansvar att leda och styra arbetet med cybersäkerhet ska minst omfatta att

1. besluta om mål och inriktning,
2. säkerställa att arbetet med att genomföra säkerhetsåtgärder bedrivs systematiskt och riskbaserat med stöd av interna regler och arbetssätt,
3. besluta om arbetsuppgifter och mandat för de roller som arbetet kräver,
4. säkerställa tillgång till kompetens för arbetet,
5. besluta om resurstilldelning,
6. besluta om kriterier för riskacceptans,
7. besluta om acceptabla tider för nedsatt funktionalitet för organisationens verksamheter,
8. besluta om prioriteringsordning för återställning av verksamheter,
9. besluta om vilka system som är sektorskritiska, och
10. övervaka genomförandet av säkerhetsåtgärder.

7 § Ledningen ska minst utse roller motsvarande samordnare, informationsägare och systemägare.

Ledningen ska ge

1. samordnaren mandat att samordna och utvärdera arbetet med säkerhetsåtgärder som stöd för ledningens arbete med cybersäkerhet,
2. informationsägaren ansvar för att information klassas och ges ett tillräckligt skydd och mandat att besluta om att påbörja behandling av information, samt
3. systemägaren ansvar för att system skyddas med lämpliga och proportionella säkerhetsåtgärder och mandat att besluta om driftsättning av system.

Ledningen ska säkerställa att information och system har en informationsägare respektive systemägare. Ledningen ska tydliggöra vilken behandling av information en informationsägare ansvarar för och vilka system som en systemägare ansvarar för.

Allmänna råd

Ledningen bör utse systemägare för organisationens olika delar i den digitala miljön.

8 § I ledningens arbete med att övervaka genomförandet av säkerhetsåtgärder ingår att vid behov men minst årligen informera sig om

1. risker som bedöms som allvarliga för cybersäkerheten,
2. status i arbetet med åtgärdsplaner,
3. betydande incidenter,
4. bristande cybersäkerhet hos leverantörer och i leveranskedjor,
5. samordnarens utvärdering enligt 2 kap. 24 §,
6. resultat av intern och extern revision,
7. resultat av genomförd tillsyn, och
8. hinder för att uppnå lämplig nivå av cybersäkerhet.

Ledningens utbildning om säkerhetsåtgärder

9 § Ledningens utbildning om säkerhetsåtgärder ska minst omfatta

1. ledningens roll i arbetet med cybersäkerhet,
2. grundläggande terminologi och relevant reglering,
3. riskhantering och övervakning som ett stöd för att leda och styra arbetet med cybersäkerhet,
4. systematiskt och riskbaserat arbete, samt
5. för ledningen relevanta interna regler, arbetssätt och stöd.

Personalsäkerhet

10 § Verksamhetsutövaren ska säkerställa att egen och inhyrd personal har förutsättningar för att behandla information och system på ett säkert sätt inför och under anställning eller uppdrag. Kontroller ska genomföras i syfte att identifiera risker med åtkomst till information och system. De ska utformas utifrån vilken information och vilka system personalen ska få åtkomst till.

Verksamhetsutövaren ska identifiera och hantera behovet av förnyade kontroller vid förändrade arbetsuppgifter.

Verksamhetsutövaren ska säkerställa att egen och inhyrd personal som avslutar anställning eller uppdrag har informerats om begränsningar av framtida användning av verksamhetsutövarens information.

Allmänna råd

Kontroller bör genomföras genom identitetskontroll, intervju, kontakt med referenser samt verifiering av akademiska, yrkesmässiga och övriga kvalifikationer.

11 § Egen och inhyrd personal ska ha relevant och aktuell kunskap och kompetens avseende cybersäkerhet för att kunna omhänderta risker vid åtkomst till information och system.
Interna regler ska minst ange

1. vilka informationsinsatser som egen och inhyrd personal ska ta del av,
2. vilka utbildningar och övningar som olika roller ska genomföra,
3. när och hur informationsinsatser, utbildningar och övningar genomförs, och
4. att tillgängliga och genomförda informationsinsatser, utbildningar och övningar följs upp och utvärderas vid behov men minst årligen.

Omvärldsbevakning
12 § Verksamhetsutövaren ska bedriva omvärldsbevakning för att kunna identifiera omständigheter och risker av betydelse för verksamhetsutövarens cybersäkerhet. I detta ingår att hålla sig uppdaterad om hot, sårbarheter, teknisk utveckling och tillgängligt stöd.

Verksamhetsutövaren ska minst bevaka

1. verksamhetsutövarens nuvarande leverantörer av hård- och mjukvara,
2. den gemensamma kontaktpunkten,
3. den nationella CSIRT-enheten,
4. det nationella cybersäkerhetscentret,
5. den nationella cyberkrishanteringsmyndigheten,
6. relevanta tillsynsmyndigheter,
7. det nationella samordningscentret för forskning och innovation inom cybersäkerhet (NCC-SE), samt
8. Europeiska unionens cybersäkerhetsbyrå (ENISA).

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

Allmänna råd

Verksamhetsutövaren bör ansluta sig till stöd för informationsutbyte om cybersäkerhet (MISP-SE) hos den nationella CSIRT-enheten.

Informationsklassning
13 § Verksamhetsutövaren ska värdera sin information avseende konfidentialitet, riktighet inklusive autenticitet, och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få.

Interna regler ska minst ange

1. att informationsägaren ansvarar för att initiera arbetet med och fastställa resultatet av informationsklassning,
2. vilka kriterier och nivåer som används vid bedömning av konsekvenser,
3. att informationsklassning genomförs innan information behandlas i system, samt
4. att resultatet av informationsklassningen följs upp och utvärderas vid behov men minst årligen.

Allmänna råd

Samma nivåer för bedömning av konsekvenser bör användas som vid värdering av risker.

Kriterier och nivåer bör utformas så att bedömningarna kan jämföras över tid.

Riskhantering

14 § Verksamhetsutövaren ska utifrån ett allriskperspektiv identifiera, analysera och värdera risker för att få underlag för valet av lämpliga och proportionella säkerhetsåtgärder.

Interna regler ska minst ange

1. att riskanalys genomförs
   a) innan information behandlas i system, och
   b) vid förändrade hot och nya sårbarheter ,
2. att uppgiften att initiera arbetet med och fastställa resultatet av riskanalysen utförs av
   a) informationsägaren avseende den information som denne ansvarar för, och
   b) systemägaren avseende de system och de delar av den digitala miljön som denne ansvarar för,
3. att resultatet av informationsklassningen och risker som identifierats genom omvärldsbevakning används som ett ingångsvärde i riskanalysen,
4. vilka kriterier och nivåer som används vid bedömning av konsekvenser och sannolikhet, samt
5. att resultatet av riskanalysen följs upp och utvärderas vid behov men minst årligen.

15 § Risker för system, segment och den digitala miljön ska identifieras, analyseras och värderas. I detta ingår att identifiera risker med

1. aggregering och ackumulering av information,
2. användning av mobila system, och
3. utkontraktering.

16 § De säkerhetsåtgärder som väljs för att åtgärda identifierade risker ska dokumenteras i en åtgärdsplan eller motsvarande. I åtgärdsplanen ska minst anges

1. vilket system, segment eller vilken del av den digitala miljön som avses,
2. vilka säkerhetsåtgärder som övervägts respektive valts,
3. motivering av valet av en säkerhetsåtgärd utifrån ledningens kriterier för riskacceptans,
4. vilken risk som en säkerhetsåtgärd avser att reducera,
5. tidpunkt för när en säkerhetsåtgärd ska vara genomförd,
6. vem som ansvarar för att en säkerhetsåtgärd genomförs, och
7. hur stor risken bedöms vara efter att säkerhetsåtgärden är genomförd.

Arbetet med säkerhetsåtgärder enligt åtgärdsplanen ska följas upp utifrån identifierat behov, men minst var tredje månad.

Incidenthantering

17 § Verksamhetsutövaren ska kunna upptäcka och vidta åtgärder för att minimera konsekvenserna av incidenter och tillbud i system.

Interna regler ska minst ange

1. hur information om incidenter och tillbud samlas in,
2. hur konsekvenserna av den inträffade incidenten bedöms,
3. hur konsekvenser av inträffade incidenter minimeras,
4. hur risken för ytterligare incidenter eller tillbud beaktas vid valet av åtgärder,
5. hur behandling av information återställs med stöd av driftsdokumentation,
6. hur åtgärder som vidtagits eller övervägts för att återställa information och system dokumenteras,
7. hur samverkan vid incidenter och tillbud med berörda leverantörer genomförs,
8. när och hur kontakt tas med den nationella CSIRT-enheten för stöd vid incidenter,
9. hur instruktioner från den nationella CSIRT-enheten omhändertas,
10. hur externa krav på rapportering av incidenter och tillbud uppfylls,
11. hur och när berörda målgrupper informeras,
12. hur verksamhetsutövaren ska uppfylla informationsskyldigheten vid betydande incidenter och betydande cyberhot,
13. när och hur inte tidigare publicerade sårbarheter i hårdvara och mjukvara rapporteras till den nationella CSIRT-enheten, samt
14. att och hur en grundorsaksanalys genomförs efter en incident om grundorsaken inte redan är känd.

Allmänna råd

Resultatet av informationsklassningen för den information som berörs av incidenten bör användas som ingångsvärde för bedömningen av incidentens konsekvens.

I arbetet med återställning bör vidtagna åtgärder, genomförda riskanalyser, beslut, samt avsteg från interna regler och arbetssätt dokumenteras.

Berörda målgrupper bör skyndsamt informeras om hur de kan agera för att minimera konsekvenser av det inträffade.

Det bör anges när en grundorsaksanalys ska genomföras efter inträffade tillbud.

Kontinuitetshantering

18 § Verksamhetsutövaren ska kunna bedriva sin verksamhet trots nedsatt funktionalitet eller otillgänglighet i system i produktionsmiljön.

Interna regler ska minst ange

1. hur konsekvenser av nedsatt funktionalitet och otillgänglighet hos system bedöms,
2. hur informationsägare ska bedöma behovet av att behandla information under störda förhållanden utifrån vad som är acceptabla tider för nedsatt funktionalitet och otillgänglighet för verksamheten,
3. hur och när alternativa arbetssätt ska användas vid störda förhållanden samt hur och när återgång till normalt arbetssätt ska göras,
4. hur återställning av system ska genomföras utifrån ledningens prioriteringsordning för återställning av verksamhet,
5. hur behov av resurser för att upprätthålla kontinuitet tillgodoses,
6. vilka krav som ska ställas på leverantörer för att tillgodose verksamhetens behov av kontinuitet,
7. hur och när stöd från cyberkrishanteringsmyndigheten ska användas, och
8. hur kontinuitet ska övas.

19 § Verksamhetsutövaren ska

1. identifiera och hantera behovet av redundanta funktioner för system i produktionsmiljön,
2. placera system som skapar redundant funktion i fysiskt åtskilda sektioner, och
3. öva återställning av sektorskritiska system vid behov men minst årligen.

20 § Verksamhetsutövaren ska identifiera och hantera behovet av kontinuitet i utvecklings-, test- och utbildningsmiljö.

Krishantering

21 § Verksamhetsutövaren ska minimera konsekvenser vid kriser orsakade av nedsatt funktionalitet i eller otillgänglighet hos system, segment, den digitala miljön eller leveranskedjor.

Interna regler ska minst ange

1. hur roller, mandat och arbetsuppgifter fördelas vid kriser med olika ursprung och konsekvenser för produktionsmiljön,
2. hur samverkan med berörda roller inom incident- och kontinuitetshantering genomförs,
3. fastställa när och hur roller som ska delta i arbetet vid en kris ska kontaktas,
4. hur stöd och instruktioner från cyberkrishanteringsmyndigheten omhändertas, och
5. hur och när arbetssätt för olika kriser ska övas.

Vid en cybersäkerhetskris ska verksamhetsutövaren på begäran av cyberkrishanteringsmyndigheten delta vid samverkanskonferenser och följa instruktionerna om hur konsekvenserna ska begränsas.

Allmänna råd

Vid krishantering bör etablerad stabsmetodik och struktur användas.

22 § Verksamhetsutövaren ska identifiera och hantera behovet av

1. att teckna avtal med leverantörer om stöd före, under och efter en kris,
2. tillgång till system för intern och extern kriskommunikation med höga krav på robusthet och tillgänglighet för informationsdelning och samverkan under kriser, samt
3. använda system för kriskommunikation som stöd för extern informationsdelning och samverkan före, under och efter en kris.

Allmänna råd

I syfte att stärka förmågan till kriskommunikation mellan olika organisationer som kan komma att påverkas vid en samhällsstörning bör verksamhetsutövaren öva att använda det webbaserade informationsdelningssystemet WIS som tillhandahålls av Myndigheten för civilt försvar.

Uppföljning och utvärdering

23 § Verksamhetsutövaren ska vid behov men minst årligen bedöma effektiviteten av införda säkerhetsåtgärder genom att följa upp och utvärdera deras lämplighet och proportionalitet i förhållande till externa krav, interna behov och risk.

Allmänna råd

Vid uppföljning och utvärdering av säkerhetsåtgärder bör etablerade metoder användas. Exempel på sådana metoder är egenkontroller, granskningar, tester samt interna och externa revisioner. Uppföljning och utvärdering bör genomföras i samband med att säkerhetsåtgärder införs. Det bör även ske vid förändrade hot eller när nya sårbarheter identifieras.

Verksamhetsutövarens systematiska och riskbaserade arbete med cybersäkerhet bör följas upp och utvärderas. Det bör omfatta hur ledningens mål och inriktning efterlevs och omfatta om interna regler, arbetssätt och stöd motsvarar verksamhetens behov. Vidare bör hinder för arbetet bedömas, till exempel brister i tilldelning av arbetsuppgifter, mandat, kompetensförsörjning eller resurser.

Uppföljning och utvärdering bör även göras vid verksamhetsuppföljning, omorganisation, förändrade rättsliga krav, inför beslut om utkontraktering samt efter betydande incidenter.

24 § Samordnaren ska utvärdera nivån på cybersäkerheten i förhållande till externa krav, interna behov och risk utifrån minst följande underlag

1. ledningens mål och inriktning,
2. genomförda informationsklassningar,
3. genomförda riskanalyser,
4. aktuella åtgärdsplaner,
5. utvärdering av säkerhetsåtgärder,
6. information om inträffade incidenter och tillbud samt genomförda grundorsaksanalyser,
7. utvärdering av cybersäkerhet hos leverantörer och i leveranskedjor, samt
8. genomförda interna och externa revisioner.

3 kap. Tekniska och driftrelaterade säkerhetsåtgärder

Förvärv, utveckling och underhåll av system

1 § Verksamhetsutövaren ska säkerställa att systemen skyddas med lämpliga och proportionella säkerhetsåtgärder genom systemens livslängd.

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, första stycket b, i 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)

Allmänna råd

Sektorskritiska system bör vara certifierade enligt EU:s cybersäkerhetsförordning (EU 2019/881).

3 § Innan avtal som innefattar att behandling av information utkontrakteras tecknas med en leverantör ska verksamhetsutövaren

1. genomföra en informationsklassning av den information som ska utkontrakteras,
2. ha åtgärdat de risker utkontrakteringen innebär,
3. säkerställa att informations- och systemägare är utsedda för den informationshantering som utkontrakteras,
4. identifierat de krav på säkerhetsåtgärder som behöver ställas på leverantören,
5. kontrollerat att tilltänkt leverantör uppfyller kraven på säkerhetsåtgärder och bedömt att leverantören kommer att kunna uppfylla kraven under avtalstiden, samt
6. säkerställa att avtalet reglerar

    a) vilka säkerhetsåtgärder leverantören ska vidta,
    b) vilken kompetens avseende cybersäkerhet leverantören behöver
    c) när och hur leverantören ska informera om förändringar i system som kan påverka avtalsefterlevnaden,
    d) hur leverantören ska informera verksamhetsutövaren om misstänkta och inträffade incidenter och tillbud,
    e) i vilken omfattning leverantören ska öva incident-, kontinuitets- och krishantering med verksamhetsutövaren,
    f) hur leverantören ska informera verksamhetsutövaren om identifierade sårbarheter,
    g) hur leverantören ska följa upp sin egen och eventuella underleverantörers efterlevnad av ställda avtalskrav på säkerhetsåtgärder att verksamhetsutövaren har rätt att följa upp efterlevnaden av ställda krav, samt
    h) hur verksamhetsutövarens information ska återlämnas eller förstöras när avtalet upphör.

Innan behandlingen av information hos leverantören påbörjas ska verksamhetsutövarens informationsägare godkänna behandlingen och verksamhetsutövarens systemägare fatta beslut om driftsättning.

4 § Inför och under utveckling av system ska verksamhetsutövaren säkerställa att

1. informationsägare och systemägare involveras i arbetet för att identifiera och hantera behov av säkerhetsåtgärder,

2. informationsklassning är genomförd och hålls uppdaterad,
3. riskanalys är genomförd och hålls uppdaterad,
4. åtgärdsplanen hålls uppdaterad, och
5. etablerade metoder för säker utveckling följs.

5 § Innan ett beslut om att för första gången driftsätta ett system ska fattas, ska systemägaren minst kontrollera att

1. det finns nödvändig dokumentation för drift och förvaltning,
2. säkerhetstester och granskningar genomförts för att säkerställa att valda säkerhetsåtgärder är lämpliga och proportionella,
3. tilldelade resurser för driften av systemet är tillräckliga,
4. informationsägaren har beslutat om att påbörja behandlingen av information, och
5. en riskanalys av identifierade brister avseende punkt 1-4 genomförts och det är dokumenterat hur dessa åtgärdas.

Systemägaren ska genomföra samma kontroller som ovan vid underhåll av system som innebär en förändring som kan påverka säkerheten i verksamhetsutövarens digitala miljöer.

6 § Innan ett beslut om avveckling av ett system fattas, ska systemägaren minst kontrollera att

1. riskanalys rörande avveckling har genomförts,
2. åtgärdsplan för avveckling finns,
3. tilldelade resurser för avveckling av systemet är tillräckliga,
4. informationsägaren beslutat om att avveckla behandlingen av informationen, och
5. en riskanalys av identifierade brister avseende punkt 1-4 genomförts och det är dokumenterat hur dessa åtgärdas.

Driftrelaterad dokumentation

7 § Verksamhetsutövaren ska upprätthålla uppdaterad dokumentation över befintlig arkitektur. Dokumentationen ska minst beskriva

1. hur den digitala miljön är indelad,
2. vad respektive del innhåller avseende

   a) segment
   b) system,
   c) hårdvara,
   d) mjukvara, och

3. aktuella informationsflöden

   e) mellan olika delar i den digitala miljön,
   f) mellan interna system, samt
   g) till och från system hos andra organisationer.

Allmänna råd

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

8 § För varje system som används i produktionsmiljön ska det finnas uppdaterad dokumentation över

1. fastställd systemägare,
2. informationsägare vars information behandlas i systemet,
3. resurser som behövs för drift och förvaltning,
4. förekomsten av information som vid informationsklassning bedömts ha behov av utökat skydd,
5. vilken egen verksamhet systemet stödjer,
6. om systemet är sektorskritiskt och på vilket sätt,
7. om systemet är nödvändigt för att upprätthålla viktiga samhällsfunktioner hos andra organisationer och på vilket sätt,
8. acceptabla tider för nedsatt funktionalitet respektive otillgänglighet,
9. vilka behov av cybersäkerhet som systemet behöver uppfylla,
10. om systemet är placerat i it-segment eller ot-segment,
11. vilken hårdvara som används och hur den identifieras samt dess version,
12. vilken mjukvara som används och dess version,
13. hur hård- och mjukvara är konfigurad,
14. hur systemet återställs,
15. aktuell riskanalys,
16. vilka säkerhetsåtgärder som genomförts för att möta identifierat behov av säkerhet, samt
17. risker som inte åtgärdats.

9 § Verksamhetsutövaren ska identifiera och hantera behovet av dokumentation för varje system i utvecklings-, test- och utbildningsmiljö.

Allmänna råd

Dokumentationen av hur hårdvara identifieras bör inkludera mac-adress och ip-adress.

10 § Det ska finnas en uppdaterad förteckning över

1. vilka system som är sektorskritiska,
2. behandling av information som är utkontrakterad och till vilken leverantör, samt
3. kontaktuppgifter till anlitade leverantörer

    a) för utkontraktering, samt

b) av hård- och mjukvara.

Verksamhetsutövaren ska identifiera och hantera behovet av att ha kontaktuppgifter till olika funktioner hos leverantören.

Kontaktuppgifter till funktioner hos leverantören som ger stöd vid incidenter ska finnas lättillgängliga för användning vid incidenthantering.

Segmentering och filtrering

11 § Verksamhetsutövaren ska dela in sin produktionsmiljö i segment för att förhindra spridning och minimera konsekvenser av incidenter. I produktionsmiljöns it-segment ska, om inte särskilda hinder identifierats, minst följande placeras i separata segment

1. klienter för användare,
2. klienter för systemadministration,
3. sektorskritiska system,
4. centrala stödfunktioner i form av skrivare, scanner och liknande,
5. centrala säkerhetsfunktioner,
6. trådlösa nätverk,
7. gästnätverk,
8. system som sammankopplas med system hos leverantör,
9. externt åtkomliga tjänster, och
10. system som innehåller sårbarheter som inte kan hanteras.

Allmänna råd

Följande centrala säkerhetsfunktioner bör placeras i separata segment

1. filtrering av extern kommunikation,
2. behörighetskontroll,
3. säkerhetsloggning,
4. säkerhetskopiering, och
5. övervakning av system.

12 § Verksamhetsutövaren ska identifiera och hantera behovet av

1. att placera varje system, ett begränsat antal system eller system med liknande funktion, användning eller skyddsbehov i separata segment, och
2. ot-segment.

Allmänna råd

Varje sektorskritiskt system bör placeras i separata segment.
Varje system i ot-segment bör placeras i separata segment.

13 § Trafik mellan segment ska filtreras så att endast godkända informationsflöden förekommer.

Trafik mellan system inom ett it-segment ska filtreras så att endast godkända informationsflöden förekommer.

14 § Utveckling, tester och utbildning som kan påverka säkerheten i produktionsmiljöns it-segment ska ske i en från produktionsmiljön avskild utvecklings-, test- respektive utbildningsmiljö.

Risker med utveckling, tester och utbildning i produktionsmiljöns ot-segment ska identifieras och åtgärdas.

Behörighetshantering och autentisering

15 § Verksamhetsutövaren ska genom behörighetshantering säkerställa att det endast är behöriga användare och system som har åtkomst till system, segment och olika delar av den digitala miljön.

Interna regler ska minst ange

1. vilken information och vilka system som får vara tillgängliga utan behörighetstilldelning,
2. hur användare och system ska identifieras,
3. hur användare och system ska tilldelas digitala identiteter och behörigheter,
4. när en digital identitet ska låsas, blockeras och tas bort,
5. när behörigheter ska ändras eller återkallas,
6. hur autentiseringsuppgifter ska utformas avseende längd och komplexitet, samt
7. hur autentiseringsuppgifter byts, distribueras och skyddas.

Allmänna råd

Interna regler för behörighetshantering bör ange

1. att en digital identitet i produktionsmiljön endast får användas av en användare eller ett system,
2. tidsbegränsningar för tilldelade digitala identiteter och behörigheter,
3. hur många misslyckade inloggningsförsök som tillåts innan en digital identitets ska låsas, och
4. att kontroll av behörighet ska genomföras innan åtkomst ges till centrala stödfunktioner i form av skrivare, scanner och liknande.

16 § Verksamhetsutövaren ska

1. säkerställa att varje digital identitet inte tilldelas behörighet till mer information eller fler system än nödvändigt,
2. säkerställa att digitala identiteter som används i produktionsmiljön inte används i utvecklings-, test- och utbildningsmiljö,
3. vid behov men minst årligen kontrollera om tilldelade digitala identiteter och behörigheter fortfarande ska kunna användas, samt

4. identifiera och hantera behovet av att använda tekniska system som stöd för efterlevnad av interna regler och arbetssätt för behörighetshantering och autentisering.

17 § Digitala identiteter som ger systemadministrativ behörighet ska endast användas för systemadministration och inte innehålla andra behörigheter. Dessa identiteter ska tidsbegränsas och tilldelas restriktivt. Systemadministrativa behörigheter som ges till en leverantör ska begränsas gällande omfattning och tid till aktuellt uppdrag. Tilldelning av andra priviligierade behörigheter ska ske restriktivt.

Allmänna råd

En digital identitet med systemadministrativ behörighet bör endast ges åtkomst till en begränsad del av produktionsmiljön.

18 § För att minimera konsekvenserna av obehörig åtkomst till behörigheter ska verksamhetsutövaren identifiera och hantera behovet av att fördela behörigheter i olika kataloger.

Allmänna råd

I produktionsmiljön bör verksamhetsutövaren använda olika kataloger för

1. it-segment,
2. ot-segment, och
3. publika tjänster som kräver inloggning.

Verksamhetsutövaren bör använda olika kataloger för utvecklings-, test- och utbildningsmiljö.

19 § Vid åtkomst till system som behandlar information som vid informationsklassning bedömts ha behov av utökat skydd ska flerfaktorsautentisering användas.

I produktionsmiljön ska flerfaktorsautentisering användas för

1. egen och inhyrd personals åtkomst via externt nätverk,
2. leverantörers åtkomst via externt nätverk, och
3. systemadministrativ åtkomst till system i nätverk.

Verksamhetsutövaren ska identifiera och hantera övrigt behov av flerfaktorsautentisering i sin digitala miljö.

20 § Verksamhetsutövaren ska identifiera och hantera behovet av att andra organisationer och enskilda personer kan verifiera verksamhetsutövaren som avsändare av information.

Allmänna råd

I arbetet med att hantera behovet av att kunna verifiera versamhetsutövaren som avsändare av information bör i e-post, sms, telefonsamtal och webbsidor omhändertas.

På sin webbplats bör verksamhetsutövaren tillhandahålla lättillgänglig information om hur andra organisationer och enskilda personer kan verifiera att det är verksamhetsutövaren som avsändare av information.

21 § Verksamhetsutövaren ska identifiera och hantera behovet av att tillhandahålla e-tjänster som kräver inloggning med e-legitimation och säkerställa tillräcklig redundans i sådana tjänster.

Säkerhetsloggning och logganalys

22 § Verksamhetsutövaren ska genom loggning säkerställa att intrång, tekniska fel och brister i cybersäkerheten kan upptäckas och utredas.

Interna regler ska minst ange

1. vilka säkerhetsrelaterade händelser som ska säkerhetsloggas,
2. tidpunkt för när säkerhetsloggning ska genomföras,
3. hur säkerhetsloggar ska utformas och vilka ytterligare uppgifter som säkerhetsloggarna ska innehålla utöver 26 §,
4. hur säkerhetsloggar ska skyddas mot obehörig åtkomst, obehörig förändring och fysisk skada,
5. var säkerhetsloggar ska lagras och hur länge de ska bevaras, samt
6. när och hur säkerhetsloggar ska analyseras och av vem.

Allmänna råd

Ett centralt systemstöd avsett för säkerhetsloggar bör användas för att samla och analysera loggarna.

23 § Försök till obehörig åtkomst och obehörig åtkomst till den digitala miljön ska loggas.

24 § Följande säkerhetsrelaterade händelser i produktionsmiljön ska minst loggas

1. åtkomst till produktionsmiljön som förutsätter tilldelad behörighet,
2. åtkomst till system som förutsätter tilldelad behörighet,
3. försök till obehörig åtkomst och obehörig åtkomst till
   a) produktionsmiljön,
   b) it- och ot-segment,
   c) system i it-segment, och
4. användning av systemadministrativ behörighet,
5. förändring av säkerhetskonfigurationer,

6. förändring av behörighet för användare och system,
7. åtkomst till information som vid informationsklassning bedömts ha behov av utökat skydd, samt
8. händelser som upptäckts genom övervakning och indikerar brister i cybersäkerheten.

25 § Verksamhetsutövaren ska identifiera och hantera behovet av säkerhetsloggning i utvecklings-, test- och utbildningsmiljö.

26 § Säkerhetsloggarna ska minst innehålla uppgift om

1. vilken användare eller vilket system som givit upphov till händelsen,
2. vilken händelse som inträffat,
3. vilken information som har påverkats, och
4. vid vilken tidpunkt händelsen inträffade.

Säkerhetsloggarna ska utformas på ett sätt som möjliggör jämförbarhet mellan olika loggar. Loggarna ska vara tillgängliga för analys under fastställd bevarandetid.

27 § Innehållet i säkerhetsloggarna ska analyseras för att upptäcka och utreda brister i cybersäkerheten.

Robust och spårbar tid

28 § Verksamhetsutövare ska använda robust och korrekt tid som är spårbar till den svenska tillämpningen av koordinerad universell tid, UTC (SP), i sin produktionsmiljö för att möjliggöra jämförbarhet av säkerhetsloggar vid incidenter som involverar andra organisationer.

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

Allmänna råd

För robust och korrekt tid bör tidstjänsten Swedish Distributed Time Service användas.

Skydd mot skadlig kod

29 § Verksamhetsutövaren ska använda mjukvara som ger skydd mot skadlig kod för system i it-segment där sådan mjukvara finns tillgänglig.

Verksamhetsutövaren ska identifiera och hantera

1. risker om mjukvara som ger skydd mot skadlig kod inte finns tillgänglig, och
2. behovet av att endast tillåta mjukvara som på förhand godkänts för installation eller användning.

Allmänna råd

För system i ot-segment bör mjukvara användas som ger skydd mot skadlig kod om sådan mjukvara finns tillgänglig.

Kryptering

30 § Verksamhetsutövaren ska identifiera och hantera behovet av kryptering för att skydda information i system mot obehörig åtkomst och obehörig förändring vid överföring och lagring.

Interna regler ska minst ange

1. hur nationella rekommendationer från det nationella cybersäkerhetscentret (NCSC) gällande kryptering omhändertas,
2. kriterier för val och godkännande av krypteringsalgoritmer, krypteringsprotokoll och nyckellängder, samt
3. när och hur krypteringsnycklar genereras, distribueras, används, återkallas och förstörs.

31 § Kryptering ska användas i verksamhetsutövarens digitala miljö för att minst skydda

1. säkerhetsloggar, och
2. autentiseringsuppgifter.

32 § Information som vid informationsklassning bedömts ha behov av utökat skydd ska skyddas med kryptering vid överföring till system utanför verksamhetsutövarens digitala miljö.

33 § Domain Name System Security Extensions (DNSSEC) ska användas för domännamn som verksamhetsutövaren registrerat i domännamnssystemet (DNS).

Säkerhetskonfigurering

34 § Verksamhetsutövaren ska skydda system mot obehörig åtkomst genom säkerhetskonfigurering. Konfigurationen ska anpassas till det behov av säkerhet som identifierats.

Som minst ska

1. förinställda autentiseringsuppgifter bytas ut, och
2. funktioner som inte behövs tas bort, stängas av eller blockeras.

Allmänna råd

Tekniska systemstöd bör användas för att införa och följa upp valda konfigurationer.

Direktkommunikation mellan klienter bör inte tillåtas ochinaktiva sessioner bör automatiskt avslutas efter en fördefinierad tidsperiod. Säkerhetsfunktioner bör konfigureras så att säkerhet upprätthålls när tekniska fel och brister inträffar.

Vid säkerhetskonfigurering bör leverantörens rekommendationer och relevanta standarder användas.

Säkerhetstester

35 § Verksamhetsutövaren ska genomföra säkerhetstester för att identifiera brister i cybersäkerheten.

Säkerhetstester ska användas för att minst kontrollera att

1. systemen är uppdaterade,
2. konfigurationer omhändertar publicerade sårbarheter, samt
3. valda tekniska säkerhetsåtgärder för system, segment och digitala miljö är genomförda och möter identifierade behov av cybersäkerhet.

Allmänna råd

Etablerad testmetodik bör användas för automatiserade respektive manuella säkerhetstester

Upptäcks sårbarheter som inte tidigare publicerats bör dessa rapporteras till den nationella CSIRT-enheten.

Säkerhetskopiering

36 § Verksamhetsutövaren ska kunna återställa information som förlorats eller förvanskats inom fastställda acceptabla tider för nedsatt funktionalitet och otillgänglighet i system.

37 § Verksamhetsutövaren ska identifiera och hantera behovet av säkerhetskopiering.

Interna regler ska minst ange

1. vilken information som ska säkerhetskopieras,
2. hur ofta och på vilket sätt säkerhetskopior ska tas,
3. hur säkerhetskopior ska skyddas och lagras,
4. hur länge säkerhetskopiorna ska bevaras,
5. hur återläsning av säkerhetskopior ska göras, och
6. hur återläsning av säkerhetskopior kontrolleras.

Säkerhetskopiorna ska skyddas mot obehörig åtkomst, obehörig förändring och fysisk skada. Minst en säkerhetskopia ska skyddas mot skadlig kod genom att lagras på hårdvara separerad från det system som informationen hämtats ifrån.

Allmänna råd

Verksamhetsutövaren bör

1. bedöma programvara, konfiguration och information separat avseende vad som ska säkerhetskopieras och hur ofta,
2. använda tekniskt systemstöd för att kontrollera att information på säkerhetskopior är korrekt och komplett, samt

3. kontrollera att information kan återställas från säkerhetskopior inom acceptabla tider för nedsatt funktionalitet och otillgänglighet vid större förändringar av produktionsmiljön men minst årligen.

Övervakning av system

38 § Verksamhetsutövaren ska använda intrångsdetektering och intrångsskydd i produktionsmiljön för att upptäcka intrång, tekniska fel, incidenter och tillbud i egna system.

Behovet av intrångsdetektering och intrångsskydd i utvecklings-, test- och utbildningsmiljö ska identifieras och hanteras.

39 § Behovet av realtidsövervakning ska identifieras och hanteras.

Allmänna råd

Realtidsövervakning bör användas i produktionsmiljön för att skyndsamt upptäcka incidenter och tillbud i centrala säkerhetsfunktioner och sektorskritiska system.

Ändringshantering

40 § Verksamhetsutövaren ska genomföra ändringar i produktionsmiljön på ett strukturerat och spårbart sätt för att minska risken för incidenter och tillbud.

Interna regler ska minst ange

1. kriterier för när och hur uppdateringar och uppgraderingar ska genomföras i it- och ot-segment, samt
2. hur beslut om att genomföra ändringar fattas så att endast godkända ändringar genomförs.

Allmänna råd

Kriterier bör fastställas för när och hur uppdateringar och uppgraderingar ska genomföras i utvecklings-, test- och utbildningsmiljö.

---

41 § Verksamhetsutövaren ska identifiera och åtgärda risker för att säkerheten påverkas när

1. system, it-segment, ot-segment och olika delar av den digitala miljön införs, uppgraderas, uppdateras och avvecklas, samt
2. uppdatering eller uppgradering inte kan genomföras i enlighet med fastställda kriterier eller pågående ändring behöver avbrytas.

42 § I it-segment ska säkerhetsuppdateringar genomföras utan onödigt dröjsmål. 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

Arbetet med att godkänna en säkerhetsuppdatering bör inledas senast inom 72 timmar efter att den tillgängliggjorts av leverantören.

Mjukvara bör uppdateras till senaste version utan onödigt dröjsmål.

4 kap. Fysiska säkerhetsåtgärder

Lokaler

1 § Verksamhetsutövaren ska skydda lokaler där information behandlas mot obehörigt tillträde för att undvika obehörig fysisk åtkomst till, förlust av och fysisk skada på system genom att minst

1. ha ett för verksamheten anpassat skalskydd, samt
2. dela in sina lokaler i fysiskt separerade sektioner utifrån resultat av informationsklassning och riskanalys avseende den information som ska behandlas i lokalerna.

2 § Verksamhetsutövaren ska identifiera och hantera behovet av

1. tillträdesbegränsning till lokaler och sektioner,
2. övervakning av lokaler och sektioner samt av att agera på larm vid obehörigt tillträde,
3. att kontrollera egen och inhyrd personals samt besökares identitet innan de ges tillträde till lokaler och sektioner,
4. särskild sektion för besökare,
5. att inrätta sektioner i form av särskilda it-utrymmen, och
6. ytterliga indelning i sektioner inom särskilda it-utrymmen.

3 § Särskilda it-utrymmen ska förses med övervakning och larm. Tillträde till särskilda it-utrymmen ska tilldelas restriktivt och registreras på individnivå.

4 § För att undvika förlust av, skada på eller funktionsavbrott i system ska verksamhetsutövaren identifiera och hantera behov av att minst skydda lokaler mot

1. brand,
2. vattenskador,
3. onormal luftfuktighet, och
4. onormal temperatur.

System

5 § Verksamhetsutövaren ska skydda system mot obehörig fysisk åtkomst, förlust och fysisk skada genom att identifiera och hantera behovet av att placera servrar och nätverksutrustning i särskilda it-utrymmen eller låsta skåp.

Servrar som används för att bedriva sektorsverksamhet ska placeras i särskilda it-utrymmen eller i låsta skåp.

Tekniska försörjningssystem

6 § Verksamhetsutövaren ska undvika förlust av eller skada på system eller avbrott i deras funktion på grund av fel eller avbrott i tekniska försörjningssystem.

Verksamhetsutövaren ska säkerställa tillräcklig funktion och redundans i produktionsmiljö avseende

1. elförsörjning,
2. elektroniska kommunikationsnät och elektroniska kommunikationstjänster,
3. kyla,
4. värme, och
5. ventilation.

7 § Verksamhetsutövaren ska identifiera och hantera behovet av att övervaka de tekniska försörjningssystemens funktion och säkerställa att larm genereras vid otillräcklig funktion vid på förhand fastställda nivåer i produktionsmiljön.

8 § Verksamhetsutövaren ska identifiera och hantera behovet av tillräcklig funktion och redundans hos tekniska försörjningssystem i utvecklings-, test- och utbildningsmiljö.

5 kap. Sektorsspecifika säkerhetsåtgärder

Offentlig förvaltning

System för kriskommunikation

1§ Verksamhetsutövaren ska identifiera och hantera behovet av att använda Rakel (Radiokommunikation för effektiv ledning) och SGSI (Swedish Government Secure Intranet) för kriskommunikation.

2 § Verksamhetsutövare ska en gång per kvartal, kontrollera funktionen hos system för intern och extern kriskommunikation.

6 kap. Undantag

Myndigheten för samhällsskydd och beredskap får i enskilda fall och om det finns särskilda skäl medge undantag från tillämpningen av dessa föreskrifter.

---

1. Dessa föreskrifter och allmänna råd träder i kraft [Klicka och skriv tidsangivelse].

Myndigheten för samhällsskydd och beredskap

MIKAEL FRISELL

Tove Wätterstam
Avdelningen för cybersäkerhet och samhällsviktiga kommunikationer

Beställningsadress:
Norstedts Juridik, 106 47 Stockholm
Telefon: 08-657 95 00
E-post: order@forlagssytem.se
Webbadress: www.nj.se/offentligapublikationer
Beställningsnummer: