Myndigheten för samhällsskydd och beredskaps författningssamling

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

MSBFS 2020:7
Utkom från trycket
den 11 september 2020

Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter;

beslutade den 1 september 2020.

Myndigheten för samhällsskydd och beredskap föreskriver följande med stöd av 21 § förordningen (2015:1052)[1] om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och beslutar följande allmänna råd[2].

1 kap. Inledande bestämmelser

Tillämpningsområde

1 § Dessa föreskrifter innehåller bestämmelser om sådana säkerhetskrav som avses i 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

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

Begreppsförklaring

3 § I dessa föreskrifter avses med

extern aktör	Leverantör som inte omfattas av dessa föreskrifter, inhyrd personal eller motsvarande.
informationssystem	Applikationer, tjänster eller andra komponenter som hanterar information. I begreppet ingår också nätverk och infrastruktur.

[1] Förordningen senast ändrad genom SFS 2020:25.
[2] 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.

it-miljö	Den samlade mängden informationssystem som används för att behandla information som myndigheten ansvarar för.
produktionsmiljö	Den del av it-miljön som myndigheten använder för att utföra sitt uppdrag.
redundant funktion	Två eller flera, identiska eller olika, funktioner som oberoende av varandra uppfyller samma syfte.
systemadministrativ behörighet	Behörighet med priviligierade rättigheter som ger möjlighet att förändra grundläggande funktioner och säkerhetsfunktioner i ett informationssystem.
säkerhetsfunktion	Funktion som svarar för viss del av säkerheten såsom behörighetskontrollsystem, säkerhetsloggning, intrångsdetektering, intrångsskydd eller skydd mot skadlig kod.
säkerhetsloggning	Elektronisk registrering av säkerhetsrelaterade händelser.

2 kap. Grundläggande bestämmelser

Ansvar

1 § Myndigheten ska, för varje informationssystem, tydliggöra vilken befattning som ansvarar för att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder (systemägare).

Omvärldsbevakning och riskbedömning

2 § Myndigheten ska bedriva omvärldsbevakning för att underlätta identifiering och hantering av hot mot och sårbarheter i myndighetens informationssystem.

3 § Myndigheten ska genomföra riskbedömning för enskilda informationssystem och myndighetens produktionsmiljö i sin helhet.

Allmänna råd

Riskbedömningar bör även genomföras för myndighetens utvecklings-, test- respektive utbildningsmiljö.

Myndigheten bör överväga att ge systemägaren för berört informationssystem i uppgift att säkerställa att riskbedömning genomförs.

Dokumentation av it-miljön

4 § Myndigheten ska upprätthålla uppdaterad dokumentation över

1. hård- och mjukvara som används i varje enskilt informationssystem,
2. beroenden mellan olika interna informationssystem respektive beroenden av informationssystem hos externa aktörer,
3. vilka informationssystem som behandlar information som har behov av utökat skydd, och
4. vilka informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag.

Allmänna råd

Tekniskt stöd bör användas för att upprätthålla uppdaterad dokumentation.
Beroenden bör tydliggöras i en systemkarta eller motsvarande.
Information som är i behov av utökat skydd bör identifieras med stöd av informationsklassning enligt 6 § MSBFS 2020:6.

3 kap. Utveckling, anskaffning och utkontraktering

Kravställning och kontroll

1 § Myndigheten ska, vid utveckling, anskaffning eller utkontraktering av informationssystem, identifiera krav på säkerhet avseende

1. uppdelning i nätverkssegment,
2. filtrering av nätverkstrafik,
3. behörigheter, digitala identiteter och autentisering,
4. kryptering,
5. säkerhetskonfigurering,
6. säkerhetstester och granskningar,
7. ändringshantering, uppgradering och uppdatering,
8. robust och korrekt tid,
9. säkerhetskopiering,
10. säkerhetsloggning och tillhörande analys,
11. övervakning av nätverkstrafik,
12. övervakning av informationssystem inklusive säkerhetsfunktioner,
13. skydd mot skadlig kod,
14. skydd av utrustning,
15. redundans och återställning,
16. kontinuitet under fredstida krissituation samt inför och vid höjd beredskap,
17. arkivering, och
18. avveckling.

Myndigheten ska dokumentera vilka säkerhetsåtgärder som valts för att möta respektive krav.

Allmänna råd

Vid anskaffning av informationssystem bör myndigheten överväga att välja produkter som är certifierade genom tredjepartsgranskning mot etablerad standard.

2 § Myndigheten ska, innan driftsättning och inför förändring som kan påverka säkerheten i informationssystemen,

1. genom säkerhetstester och granskning kontrollera att valda säkerhetsåtgärder är tillräckliga för att möta identifierade krav på säkerhet, och
2. verifiera att det finns nödvändig dokumentation för drift och förvaltning.

I de fall brister identifieras ska myndigheten riskbedöma och hantera dessa brister innan driftsättning eller inför förändring som kan påverka säkerheten i informationssystemen.

Allmänna råd

Nödvändig dokumentation för drift och förvaltning bör omfatta arkitektur, ingående komponenter, konfiguration, dataflöden och övrig relevant systeminformation. Av dokumentationen bör även framgå vem som är systemägare samt om och till vilken extern aktör informationssystemet är utkontrakterat.

Utvecklings-, test- och utbildningsmiljöer

3 § Myndighetens arbete med utveckling och tester som kan påverka informationssäkerheten i produktionsmiljön ska ske i en från produktionsmiljön avskild del av it-miljön.

4 § Myndigheten ska identifiera och hantera behovet av en utbildningsmiljö som är avskild från produktionsmiljön.

4 kap. Drift och förvaltning

Uppdelning i nätverkssegment och filtrering av nätverkstrafik

1 § Myndigheten ska förhindra spridning av incidenter och minska konsekvenser av angrepp genom att placera informationssystem med olika funktioner i separata nätverkssegment i sin produktionsmiljö.

Allmänna råd

Följande funktioner i produktionsmiljön bör placeras i separata nätverkssegment:

1. Klienter för användare.
2. Klienter för administration.
3. Servrar.
4. Centrala systemsäkerhetsfunktioner i form av behörighetskontrollsystem, säkerhetsloggning, filtrering och liknande.
5. Centrala stödfunktioner i form av skrivare, scanner och liknande.
6. Trådlösa nätverk.
7. Gästnätverk.
8. Externt åtkomliga tjänster.
9. Informationssystem som sammankopplas med informationssystem hos extern aktör.
10. Industriella informations- och styrsystem.
11. System som innehåller sårbarheter som inte kan hanteras.

2 § Myndigheten ska filtrera nätverkstrafiken så att endast nödvändiga dataflöden förekommer mellan olika nätverkssegment.

Behörigheter, digitala identiteter och autentisering

3 § Myndigheten ska säkerställa att endast behöriga användare och informationssystem har åtkomst till it-miljön och utforma sin behörighetshantering på ett sådant sätt att varje digital identitet inte har mer åtkomst till information och informationssystem än vad den behöver.

Allmänna råd

Behörighetshanteringen bör säkerställa att

1. digitala identiteter i produktionsmiljön är unika,
2. digitala identiteter och behörigheter är godkända innan de kopplas till en användare eller ett informationssystem,
3. tilldelade behörigheter är tidsbegränsade och kontrolleras en gång per år,
4. behovet av att använda olika kataloger för digitala identiteter och behörigheter är identifierat och hanterat, och
5. olika digitala identiteter används vid åtkomst till utvecklings- och testmiljö respektive produktionsmiljö.

En digital identitet bör endast användas av en individ.

Digitala identiteter och behörigheter som ger tillgång till externt åtkomliga informationssystem samt utvecklings-, test- och utbildningsmiljö bör hanteras i olika kataloger skilda från kataloger för produktionsmiljön.

4 § Digitala identiteter som ger systemadministrativ behörighet ska endast användas för systemadministration och tilldelas restriktivt.

Allmänna råd

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

5 § Flerfaktorsautentisering ska användas vid

1. egen och inhyrd personals åtkomst till produktionsmiljön via externt nätverk,
2. systemadministrativ åtkomst till informationssystem, och
3. åtkomst till informationssystem som behandlar information som bedömts ha behov av utökat skydd.

6 § Myndigheten ska ha interna regler för hantering av autentiseringsuppgifter med krav på

1. längd och komplexitet,
2. när byte ska ske,
3. hur distribution ska ske, och
4. hur autentiseringsuppgifterna ska skyddas.

Allmänna råd

Tekniska system bör användas för att stödja efterlevnaden av reglerna avseende längd, komplexitet och byte.

Kryptering

7 § Myndigheten ska identifiera och hantera behovet av kryptering för att skydda information mot obehörig åtkomst och obehörig förändring vid överföring och lagring.

Allmänna råd

Kryptering bör användas för att skydda

1. säkerhetsloggar mot obehörig åtkomst och obehörig förändring,
2. autentiseringsuppgifter mot obehörig åtkomst och obehörig förändring, och
3. information i behov av utökat skydd mot obehörig åtkomst och obehörig förändring vid överföring till informationssystem utanför myndighetens kontroll.

..Myndigheten bör identifiera behovet av att kryptera e-post på transportlagret i enlighet med OSI-modellen (Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model, ISO/IEC 7498-1) eller motsvarande. Myndigheten bör också införa möjlighet att använda sådan kryptering vid överföring av e-post till och från andra statliga myndigheter.

Myndigheten bör införa möjlighet att verifiera myndigheten som avsändare respektive mottagare av e-post.

8 § Myndigheten ska använda Domain Name System Security Extensions (DNSSEC) avseende samtliga domännamn som myndigheten registrerat i domännamnssystemet (DNS).

9 § Myndigheten ska ha interna regler för kryptering med krav på

1. hantering av krypteringsnycklar,
2. godkännande och förvaltning av krypteringslösningar, och
3. hur krypteringsalgoritmer, krypteringsprotokoll och nyckellängder ska väljas.

Säkerhetskonfigurering

10 § Myndigheten ska, för att skydda informationssystem mot obehörig åtkomst,

1. byta ut förinställda autentiseringsuppgifter,
2. stänga av, ta bort eller blockera systemfunktioner som inte behövs, och
3. i övrigt anpassa konfigurationer för att uppnå avsedd säkerhet.

Säkerhetstester och granskningar

11 § Myndigheten ska säkerställa att säkerhetstester och granskningar möjliggör identifiering av sårbarheter. Myndigheten ska ha interna regler för hur kontroll görs av att

1. informationssystemen är uppdaterade,
2. valda säkerhetsåtgärder är införda på korrekt sätt, och
3. genomförda säkerhetskonfigurationer är tillräckliga.

Allmänna råd

Automatiserade säkerhetstester och manuella granskningar bör kombineras vid kontroll av säkerheten i informationssystemen.

Ändringshantering, uppgradering och uppdatering

12 § Myndigheten ska säkerställa att förändringar i informationssystem genomförs på ett strukturerat och spårbart sätt. Myndigheten ska ha interna regler för ändringshantering med krav på

1. vilka kriterier som ska användas för att godkänna hård- och mjukvara innan installation eller användning,
2. hur risker för incidenter och avvikelser i samband med förändring i produktionsmiljön ska identifieras och hanteras,
3. hur mjukvara, utan onödigt dröjsmål, ska uppdateras till senaste version,
4. hur utbyte eller uppgradering av hård- och mjukvara som inte längre uppdateras eller stöds av leverantören ska säkerställas utan onödigt dröjsmål, och
5. hur risker ska hanteras när uppdatering eller uppgradering enligt punkt 3 och 4 inte kan genomföras.

Allmänna råd

Säkerhetsuppdateringar bör införas skyndsamt och behovet av att automatisera uppdateringar bör övervägas.

För att undvika störning vid förändring bör myndigheten genomföra tester och ta fram en plan för återställning innan förändringen genomförs.

De interna reglerna bör tydliggöra hur risker för incidenter och avvikelser i samband med förändringar i utvecklings-, test- och utbildningsmiljö identifieras och hanteras.

Korrekt och spårbar tid

13 § Myndigheten ska använda robust och korrekt tid spårbar till den svenska tillämpningen av koordinerad universell tid, UTC(SP), i sin produktionsmiljö.

Allmänna råd

..Myndigheten bör använda tidstjänsten Swedish Distributed Time Service på www.ntp.se.

Behovet av att använda robust och korrekt tid spårbar till den svenska tillämpningen av koordinerad universell tid, UTC (SP) i utvecklings-, test- och utbildningsmiljö bör identifieras och hanteras.

Säkerhetskopiering

14 § Myndigheten ska, för att kunna återställa information som förlorats eller förvanskats, regelbundet säkerhetskopiera sin information.

Allmänna råd

Myndigheten bör

1. en gång per dygn säkerhetskopiera information som behövs för myndighetens förmåga att utföra sitt uppdrag, och
2. en gång per år, eller vid större förändringar av produktionsmiljön, verifiera förmågan att, inom för myndigheten godtagbar tidsperiod, återställa information från säkerhetskopior.

Vid bedömning av säkerhetskopieringens omfattning och intervall, bör programvara, konfiguration respektive information hanteras separat.

Behovet av säkerhetskopiering och förmåga till återställning av information i utvecklings-, test- och utbildningsmiljö bör identifieras och hanteras.

15 § Säkerhetskopior ska förvaras skilda från produktionsmiljön och skyddas mot skada, obehörig åtkomst och obehörig förändring.

Säkerhetsloggning och övervakning

16 § Myndigheten ska, för att säkerställa spårbarhet i informationssystem, logga följande säkerhetsrelaterade händelser:

1. Obehörig åtkomst och försök till obehörig åtkomst till it-miljö och enskilda informationssystem.
2. Förändringar av konfigurationer och säkerhetsfunktioner som förutsätter priviligierade rättigheter.
3. Förändringar av behörighet för användare och informationssystem.
4. Åtkomst till information som bedömts ha behov av utökat skydd.

17 § Myndigheten ska analysera innehållet i säkerhetsloggarna för att upptäcka och hantera incidenter och avvikelser. Säkerhetsloggarna ska

1. möjliggöra utredning av intrång, tekniska fel och brister i säkerheten,
2. utformas på ett sätt som möjliggör jämförbarhet mellan olika loggar, och
3. vara tillgängliga för analys under fastställd bevarandetid.

Myndigheten ska dokumentera hur säkerhetsloggarna ska användas samt var loggningsuppgifter hämtas och lagras, hur de skyddas och hur länge de ska bevaras.

Allmänna råd

En säkerhetslogg bör innehålla uppgift om vem eller vad som agerat, vad som har skett och vid vilken tidpunkt.

För att skapa jämförbarhet bör myndigheten använda myndighetens tidstjänst för samtliga säkerhetsloggar.

Säkerhetsloggar bör samlas i ett för ändamålet avsett informationssystem.

18 § Myndigheten ska identifiera och hantera behovet av intrångsdetektering och intrångsskydd.

Allmänna råd

Behovet av intrångsdetektering och intrångsskydd bör bedömas för enskilda informationssystem och för myndighetens produktionsmiljö i sin helhet. Behovet bör även bedömas för myndighetens utvecklings- test- och utbildningsmiljö.

19 § Myndigheten ska identifiera och hantera behovet av realtidsövervakning av informationssystem.

Skydd mot skadlig kod

20 § Myndigheten ska använda mjukvara som ger skydd mot skadlig kod. För informationssystem där sådan mjukvara inte finns tillgänglig ska andra åtgärder vidtas som ger motsvarande skydd.

Skydd av utrustning

21 § Myndigheten ska skydda den utrustning som informationssystem består av mot skador och obehörig åtkomst, genom att

1. placera centrala servrar och central nätverksutrustning i särskilda it-utrymmen,
2. tilldela behörighet till särskilda it-utrymmen restriktivt,
3. identifiera och hantera behovet av övervakning och larm i särskilda it-utrymmen,
4. registrera tillträde till särskilda it-utrymmen på individnivå och spara dokumentationen under fastställd bevarandetid, och
5. ha interna regler för hur mobil utrustning ska skyddas.

Redundans och återställning

22 § Myndigheten ska, för att säkerställa tillgänglighet till information och informationssystem vid incidenter och avvikelser,

1. ha interna regler för återställning av produktionsmiljön i sin helhet och för enskilda informationssystem,
2. öva återställning av informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag, och
3. placera centrala servrar och central nätverksutrustning som skapar redundant funktion i olika särskilda it-utrymmen.

Allmänna råd

Övning av återställning bör ske regelbundet och utifrån identifierat behov av tillgänglighet.

5 kap. För myndigheter med ett särskilt ansvar för krisberedskapen

1 § De myndigheter som har ett särskilt ansvar för krisberedskapen enligt 10 § förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska, utöver vad som framgår av kapitel 2 – 4 i dessa föreskrifter,

1. använda flerfaktorsautentisering och realtidsövervakning för informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag, och
2. en gång per kvartal verifiera förmågan till återställning av dessa system.

2 § Myndigheten ska, en gång per kvartal, kontrollera funktionen hos informationssystem som ska användas för informationsdelning under fredstida krissituationer.

Allmänna råd

..Myndigheten bör använda Swedish Government Secure Intranet (SGSI) och Radiokommunikation för effektiv ledning (RAKEL) som stöd för informationsdelning under fredstida krissituationer.

6 kap. Undantag

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

Ikraftträdande och övergångsbestämmelser

Dessa föreskrifter träder i kraft den 1 oktober 2020.
Åtgärder i 4 kap 1 § (nätverkssegmentering), 5 § (flerfaktorsautenticering), 19 § (realtidsövervakning), 21 § (skydd av utrustning), och 5 kapitlet 1 § ska vara införda senast den 1 oktober 2021.

Myndigheten för samhällsskydd och beredskap

DAN ELIASSON

Helena Andersson
(Avdelningen för cybersäkerhet och säker kommunikation)

Beställningsadress:
Norstedts Juridik, 106 47 Stockholm
Telefon: 08-598 191 90
E-post: kundservice@nj.se
Webbadress: www.nj.se/offentligapublikationer
Beställningsnummer: 19120-07