Myndigheten för samhällsskydd och beredskaps författningssamling

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

MSBFS 2020:6
Utkom från trycket
den 11 september 2020

Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet 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].

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

behandling	En åtgärd eller kombination av åtgärder beträffande information, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

[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.

gapanalys	Identifiering av skillnaden mellan införda säkerhetsåtgärder och identifierat behov av säkerhetsåtgärder.
informationssäkerhet	Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.
ledningssystem för informationssäkerhet	Del av myndighetens övergripande ledningssystem, baserat på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och utveckla organisationens informationssäkerhet.

Systematiskt och riskbaserat informationssäkerhetsarbete

4 § Myndigheten ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna *SS-EN ISO/IEC 27001:2017 Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav* och *SS-EN ISO/IEC 27002:2017 Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder* eller motsvarande.

Allmänna råd

Om myndigheten väljer att använda en annan standard bör myndigheten analysera och dokumentera de likheter och skillnader som finns mellan ISO-standarden och vald standard för att säkerställa att vald standard ger tillräckligt stöd i det systematiska och riskbaserade informationssäkerhetsarbetet.

Hur informationssäkerhetsarbetet ska utformas

5 § Informationssäkerhetsarbetet ska utformas utifrån de risker och behov myndigheten identifierar. Det ska omfatta all behandling av information som myndigheten ansvarar för och integreras med myndighetens befintliga sätt att leda och styra sin organisation.

När myndigheten utformar informationssäkerhetsarbetet ska den

1. säkerställa att det finns en informationssäkerhetspolicy där ledningens målsättning med och inriktning för informationssäkerhetsarbetet framgår,
2. tydliggöra myndighetsledningens och den övriga organisationens ansvar, inklusive den eller de som utses att leda och samordna informationssäkerhetsarbetet, och ge dessa befattningar de befogenheter som behövs,
3. säkerställa att informationssäkerhetsarbetet tilldelas nödvändiga resurser,
4. upprätta de interna regler, arbetssätt och stöd som behövs, och
5. säkerställa att innehållet i myndighetens interna regler, arbetssätt och stöd utvärderas samt vid behov anpassas.

Utformningen av informationssäkerhetsarbetet ska dokumenteras.

Allmänna råd

Myndigheten bör tydliggöra vilka befattningar som är ansvariga för att säkerställa att information skyddas på avsett sätt (informationsägare).

Den eller de som utses att leda och samordna informationssäkerhetsarbetet bör ges en oberoende, kravställande och granskande roll.

Myndigheten bör utvärdera hur interna regler, arbetssätt och stöd svarar mot identifierade risker och behov. Utvärdering bör ske regelbundet och vid behov, såsom i samband med verksamhetsuppföljning, omorganisation, förändrade rättsliga krav och inför beslut att låta myndighetens information behandlas av en annan statlig myndighet eller en extern aktör.

Utvärderingen bör ske genom interna kontroller, granskningar, interna och externa revisioner eller motsvarande. Interna regler och arbetssätt bör tydliggöra hur och när utvärdering ska ske.

Hur informationssäkerhetsarbetet ska bedrivas

6 § Myndigheten ska säkerställa att informationssäkerhetsarbetet är systematiskt och riskbaserat genom att

1. klassa sin information avseende konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få (informationsklassning),
2. identifiera, analysera och värdera risker för sin information (riskbedömning),
3. utifrån genomförd informationsklassning och riskbedömning identifiera behov av och införa ändamålsenliga och proportionella säkerhetsåtgärder, och
4. utvärdera säkerhetsåtgärderna och vid behov anpassa skyddet av informationen. I arbetet ingår att genomföra en gapanalys.

Informationssäkerhetsarbetet och införda säkerhetsåtgärder ska dokumenteras.

Allmänna råd

Myndigheten bör som stöd för arbetet med informationsklassning och riskbedömning fastställa

1. vilka befattningar som ansvarar för att informationsklassning och riskbedömning genomförs,
2. när och i vilka situationer informationsklassning och riskbedömning ska genomföras, och
3. kriterier och nivåer för bedömning av konsekvens.

Myndigheten bör använda samma kriterier och nivåer för bedömning av konsekvens vid informationsklassning och riskbedömning. Kriterierna och nivåerna bör utformas så att bedömningarna ger resultat som kan jämföras över tid.

Myndighetens behov av spårbarhet samt autenticitet hos informationen liksom informationens behov av bevarande över tid bör beaktas vid informationsklassning.

Myndigheten bör bedöma vilka risker det medför när information som myndigheten ansvarar för ackumuleras eller aggregeras.

Vid val av ändamålsenliga och proportionella säkerhetsåtgärder bör myndigheten kombinera organisatoriska, administrativa, fysiska och tekniska åtgärder.

För att underlätta informationssäkerhetsarbetet bör myndigheten gruppera beslutade säkerhetsåtgärder i skyddsnivåer och koppla dem till informationsklassningens konsekvensnivåer. Förmågan att med beslutade skyddsåtgärder upprätthålla tillräckligt skydd på respektive skyddsnivå bör regelbundet utvärderas och vid behov utvecklas och anpassas.

När annan statlig myndighet eller en extern aktör behandlar myndighetens information

7 § I de fall myndigheten överlåter åt en annan statlig myndighet att fullgöra uppgifter som regleras i dessa föreskrifter ska myndigheterna komma överens om och dokumentera vad respektive myndighet ansvarar för samt hantera de risker överlåtelsen innebär.

Myndighetens ansvar för att klassa sin information enligt 6 § p.1 kan inte överlåtas.

8 § Myndigheten ska, innan den låter en extern aktör behandla information, utifrån informationsklassning och riskbedömning, hantera de risker en sådan behandling innebär. Myndigheten ska i avtal ställa krav på vilka säkerhetsåtgärder den externa aktören ska vidta och hur myndigheten följer upp dessa krav.

Allmänna råd

Avtalet mellan myndigheten och den externa aktören bör reglera

1. att den externa aktören ska ha tillräcklig kompetens avseende informationssäkerhet,
2. hur den externa aktören ska överlämna information till myndigheten om misstänkta eller inträffade incidenter, avvikelser och sårbarheter,
3. hur den externa aktören ska följa upp sitt egna och eventuella underleverantörers systematiska och riskbaserade informationssäkerhetsarbete, och
4. hur myndighetens information ska återlämnas när avtalet upphör.

Säkerhetsåtgärder avseende behandling av information

Åtgärder för att säkerställa att personal behandlar information på ett säkert sätt

9 § Myndigheten ska

1. anpassa bakgrundskontroller av egen och inhyrd personal utifrån vilken information personalen ska få åtkomst till,
2. hålla egen och inhyrd personal informerad om relevanta interna regler, arbetssätt och stöd,
3. utvärdera att interna regler, arbetssätt och stöd används på avsett sätt,
4. säkerställa att egen och inhyrd personal med utpekade roller i informationssäkerhetsarbetet har tillräcklig kompetens för att kunna utföra sina arbetsuppgifter, och
5. utveckla och upprätthålla kompetens hos egen personal avseende informationssäkerhet genom utbildning, informationsinsatser och övning.

Allmänna råd

Bakgrundskontroller bör ske genom intervju, kontakt med referenser samt verifiering av akademiska, yrkesmässiga och övriga kvalifikationer.

Åtgärder för att försvåra obehörig tillgång till information i myndighetens lokaler

10 § Myndigheten ska identifiera och hantera behovet av

1. skalskydd och tillträdesbegränsning för sina lokaler,
2. tekniska system för att larma vid obehörigt tillträde till sina lokaler, och
3. att dela in sina lokaler i fysiskt separerade zoner.

Åtgärder för att hantera incidenter och avvikelser

11 § Myndigheten ska ha förmåga att

1. skyndsamt upptäcka och bedöma incidenter och avvikelser,
2. återställa manipulerad eller förlorad information, och
3. bedöma om inträffad incident ska rapporteras externt.

12 § Om en incident eller avvikelse inträffat ska myndigheten identifiera grundorsaker till incidenten eller avvikelsen och vidta åtgärder för att motverka att liknande incidenter och avvikelser inträffar på nytt.

Allmänna råd

Inträffade incidenter och avvikelser bör föranleda översyn av det systematiska och riskbaserade informationssäkerhetsarbetet inklusive införda säkerhetsåtgärder. I syfte att utveckla skyddet av information bör den eller de som utsetts att leda och samordna informationssäkerhetsarbetet hos myndigheten ha åtkomst till information om inträffade incidenter och avvikelser.

Åtgärder för att upprätthålla kontinuitet under incidenter och kriser

13 § Myndigheten ska,

1. identifiera och hantera behovet av kontinuitet för behandling av information, och
2. öva förmåga att upprätthålla identifierat behov av kontinuitet.

Allmänna råd

Myndigheten bör i sitt kontinuitetsarbete

1. omhänderta tillgänglighetskraven från genomförd informationsklassning,
2. identifiera myndighetens behov av uthållighet över tid,
3. beakta behovet av att tillämpa alternativa arbetssätt, och
4. tydliggöra hur beslut om att tillämpa alternativa arbetssätt respektive beslut om att återgå till normal verksamhet fattas.

Kontinuitetsarbetet bör utvärderas

1. efter genomförda övningar,
2. vid organisationsförändringar,
3. när information överlämnas till annan statlig myndighet eller extern aktör,
4. vid förändring av rättslig reglering eller verksamhetskrav, och
5. om brister upptäcks i samband med att alternativa arbetssätt används.

Uppföljning av informationssäkerhetsarbetet

14 § Myndigheten ska minst en gång per år följa upp att informationssäkerhetsarbetet svarar mot myndighetsledningens målsättning och inriktning, genom att sammanställa och analysera resultatet av genomförda

1. utvärderingar av interna regler, arbetssätt och stöd enligt 5 § p. 5,
2. informationsklassningar enligt 6 § p. 1,
3. riskbedömningar enligt 6 § p. 2,
4. utvärderingar av säkerhetsåtgärder enligt 6 § p. 4, och
5. utvärderingar av att interna regler, arbetssätt och stöd används på avsett sätt enligt 9 § p. 3.

Allmänna råd

Uppföljningen av myndighetens informationssäkerhetsarbete bör hållas samman av den eller de som utsetts att leda och samordna informationssäkerhetsarbetet vid myndigheten.

15 § Myndighetsledningen ska informera sig om

1. i vilken utsträckning införda säkerhetsåtgärder motsvarar myndighetens behov,
2. allvarliga risker som inte åtgärdats, och
3. övriga hinder för att uppnå ledningens målsättning med och inriktning för informationssäkerhetsarbetet.

Allmänna råd

Bedömningen av övriga hinder bör inkludera brister avseende tilldelning av ansvar, resurser, mandat och befogenheter samt brister avseende interna regler och arbetssätt.

Undantag

16 § 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 då Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd (MSBFS 2016:1) om statliga myndigheters informationssäkerhet upphör att gälla.

Åtgärder enligt 10 § 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: 19120-06