Myndigheten för samhällsskydd och beredskaps författningssamling

Utgivare: Key Hedström, Myndigheten för samhällsskydd och beredskap
ISSN 2000-1886

MSBFS 2016:1
Utkom från trycket
den 11 mars 2016

Myndigheten för samhällsskydd och beredskaps föreskrifter[1] om statliga myndigheters informationssäkerhet;

beslutade den 1 mars 2016.

Myndigheten för samhällsskydd och beredskap föreskriver följande med stöd av 21 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Tillämpningsområde

1 § Denna författning innehåller föreskrifter som ansluter till bestämmelserna om statliga myndigheters informationssäkerhet i 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

2 § Om det i en annan författning finns någon bestämmelse om statliga myndigheters informationssäkerhet som avviker från denna författning, gäller den bestämmelsen.

3 § I 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap finns föreskrifter om varje myndighets ansvar för säker informationshantering. Ansvaret gäller även när myndighetens information hanteras av en extern aktör eller när myndigheten tillhandahåller andra aktörer tjänster för informationshantering inom e-förvaltning eller motsvarande.

I de fall en myndighet anlitar en annan myndighet för att fullgöra uppgifter som regleras i denna författning ska de berörda myndigheterna tydligt dokumentera sitt samarbete. Det ska i dokumentationen tydliggöras vilken myndighet som är ansvarig för att uppfylla kraven som ställs i denna författning. Informationsklassning enligt 9 § p.1 ska utföras av den myndighet som äger informationen.

[1] Allmänna råd som ansluter till föreskrifterna finns på sid 5.

Begreppsförklaring

4 § I denna författning avses med

informationsklassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss informationsmängd.
informationsmängd	Information som är avgränsad för ett visst ändamål.
informationssäkerhet	Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.
ledningssystem för informationssäkerhet	Ett sätt för organisationens ledning att på ett systematiskt sätt styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering.

Ledningssystem för informationssäkerhet

5 § Varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. I detta arbete ska standarderna ISO/IEC 27001:2014 och ISO/IEC 27002:2014 beaktas. Tillräckliga resurser ska tilldelas för informationssäkerhetsarbetet samt löpande och regelbunden information lämnas till myndighetsledningen.

6 § Ledningssystemet ska utformas utifrån verksamhetens behov och vara styrande för all hantering av information som myndigheten ansvarar för.

Genom ledningssystemet ska myndigheten

1. tydliggöra myndighetsledningens och den övriga organisationens ansvar för myndighetens informationssäkerhetsarbete,
2. tilldela nödvändiga befogenheter för de roller som arbetet med informationssäkerhet kräver, detta gäller särskilt för den eller de som ska utses för att leda och samordna arbetet,
3. säkerställa att informationssäkerhetsarbetet bedrivs samordnat samt att det regelbundet utvärderas och löpande utvecklas.

Närmare krav på myndigheternas informationssäkerhetsarbete

7 § Myndigheten ska upprätta en informationssäkerhetspolicy, andra styrande dokument samt den dokumentation som i övrigt krävs för att kunna bedriva ett ändamålsenligt arbete med myndighetens informationssäkerhet. Av informationssäkerhetspolicyn ska ansvarsfördelningen för verksamhetens informationsmängder framgå.

8 § Myndigheten ska eftersträva en god säkerhetskultur där alla i organisationen har kunskap om och förståelse för behoven av säker informationshantering, genom att

1. informera medarbetare om krav på säker informationshantering och relevanta regler inom området,
2. regelbundet, och enligt en beslutad utbildningsplan, genomföra utbildningar rörande informationssäkerhet som är anpassade till medarbetarnas uppgifter, samt
3. regelbundet, och enligt en beslutad övningsplan, genomföra övningar för att pröva och utveckla myndighetens säkerhetsåtgärder för kontinuitetshantering avseende informationssäkerhet.

9 § I syfte att hantera hot och risker som rör informationssäkerheten i verksamheten ska myndigheten med stöd av modeller som myndigheten beslutar

1. klassa information med utgångspunkt i konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser som kan uppstå av ett bristande skydd,
2. identifiera, analysera och bedöma hot och risker för verksamhetens information, system och tjänster,
3. utifrån informationsklassningens resultat och genomförd riskanalys identifiera och vidta de åtgärder som krävs för att uppfylla skyddsbehovet,
4. följa upp och utvärdera vidtagna åtgärder och gjorda bedömningar av hot och risker,
5. kontinuerligt utveckla skyddet för att över tid upprätthålla informationens behov av säkerhet, samt
6. fortlöpande dokumentera vidtagna åtgärder enligt denna paragraf.

Av de beslutade modellerna ska det bland annat framgå vid vilka tidpunkter och i vilka situationer som myndigheten genomför informationsklassning och analys av hot och risker, samt vem som ansvarar för åtgärderna. De beslutade modellerna ska vara kända av de som berörs i organisationen.

Särskilt om intern incidenthantering och kontinuitetshantering

10 § Myndigheten ska ha rutiner för att identifiera, rapportera, bedöma, hantera och dokumentera incidenter som kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation. Myndigheten ska ha rutiner för att lära av sådana inträffade incidenter och utförda åtgärder.

11 § Myndigheten ska ha rutiner för kontinuitetshantering som tydliggör hur verksamhetens informationshantering upprätthålls vid större störningar och avbrott. Förhållanden som kan uppstå i samband med fredstida kriser och under höjd beredskap ska beaktas.

Denna författning träder i kraft den 4 april 2016, då Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2009:10) om statliga myndigheters informationssäkerhet ska upphöra att gälla.

Myndigheten för samhällsskydd och beredskap

HELENA LINDBERG

Helena Andersson
(Avdelningen för utveckling av samhällsskydd)

MSBFS 2016:1

Myndigheten för samhällsskydd och beredskaps allmänna råd om statliga myndigheters informationssäkerhet

Följande allmänna råd ansluter till Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet. Termer och uttryck som används i föreskrifterna har samma betydelse här.

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

Allmänna råd är markerade med grå bakgrund.

Myndigheten för samhällsskydd och beredskap

CECILIA NYSTRÖM

Helena Andersson
(Avdelningen för utveckling av samhällsskydd)

Kommentarer till 1 - 3 §§

Dessa föreskrifter reglerar myndigheternas arbete med informationssäkerhet. Informationssäkerhetsarbetet syftar till att hindra obehörig åtkomst, säkerställa tillgänglighet vid behörig användning samt att informationen inte förändras eller förstörs på ett obehörigt sätt. Det ska även vara möjligt att spåra vem som har gjort vad och när med informationen.

Att en extern aktör är involverad i organisationens informationshantering innebär ofta ett behov av att vidta särskilda åtgärder för att upprätthålla avsedd nivå av informationssäkerhet. Med extern aktör avses andra statliga myndigheter, leverantör av myndighetsgemensamma tjänster inkluderat olika typer av direktåtkomst och e-förvaltningstjänster, utkontraktering av verksamhet eller informationshantering, inhyrda konsulter och motsvarande.

När uppdrag att hantera myndighetens information ges till extern aktör bör myndigheten analysera de säkerhetsåtgärder som ska vidtas av myndigheten själv och de krav som ska ställas på den externa aktören.

Vissa myndigheter kan, exempelvis på grund av att de är mycket små, behöva samverka med en annan myndighet (en värdmyndighet) när det gäller att utföra det praktiska arbetet med informationssäkerhet eller informationshantering i sin helhet. Myndigheten kan då överlåta till värdmyndigheten att helt eller delvis fullgöra de uppgifter som åligger myndigheten enligt dessa föreskrifter.

Kommentarer till 5 §

Stöd för hur ett ledningssystem för informationssäkerhet (LIS) kan införas och utformas finns även på www.informationssäkerhet.se, ytterligare stöd för informationssäkerhetsarbete finns på www.msb.se.

Kommentarer till 6 §

Myndighetens ledning har ansvar för att styra och skapa förutsättningar för myndighetens informationssäkerhetsarbete. Denna uppgift förutsätter uppdaterad kunskap om organisationens behov av och förutsättningar för säker hantering av information.

Myndighetens ledning bör följa upp och utvärdera informationssäkerhetsarbetet flera gånger per år.

Utvärdering bör särskilt ske i samband med mer omfattande omorganisationer, förändringar av it-infrastrukturen eller andra motsvarande förändringar där skäl finns att misstänka att informationssäkerheten kan påverkas.

Kommentarer till 7 §

Ett systematiskt och kontinuerligt informationssäkerhetsarbete förutsätter ett antal olika styrande dokument. Dokumentens övergripande syfte är att styra och stödja arbetet med att införliva informationssäkerhet i verksamhetens arbetssätt, processer, system och tjänster. Informationssäkerhetspolicyn och andra styrande dokument utgör dokumentationen av LIS.

Myndighetens dokumentation av informationssäkerhetsarbetet bör utgöra en del av den löpande informationen till myndighetsledningen och utgöra ett av underlagen vid myndighetens uppföljning och utvärdering.

En informationssäkerhetspolicy bör innehålla en beskrivning av verksamhetens behov av informationssäkerhet samt mål och övergripande principer för hur informationssäkerheten i verksamheten ska vara utformad, upprätthållas och utvecklas.

Myndighetens informationssäkerhetspolicy bör utgå från verksamhetens inriktning, organisation, intressent- och författningskrav samt identifierade hot och risker.

Styrande dokument bör upprättas i den omfattning som krävs för en kontinuerlig ledning och styrning av verksamhetens informationssäkerhet. De styrande dokumenten bör tydliggöra kraven på dokumentation av hur informationssäkerhetsarbetet bedrivs.

Myndigheten bör säkerställa att informationssäkerhetspolicyn och de styrande dokumenten kommuniceras till berörd personal, inklusive berörda externa parter.

Kommentarer till 8 §

En god säkerhetskultur innebär i korthet att medarbetarna känner sig delaktiga i, är motiverade för och har förståelse för hur och varför informationssäkerhetsarbetet bedrivs.

Myndighetens ledning bör tydliggöra kopplingen mellan säker informationshantering och möjligheten att utföra organisationens uppgifter för medarbetarna.

God säkerhetskultur avseende informationssäkerhet förutsätter att medarbetare känner till och medverkar till att gällande regelverk följs. Åtgärder som utbildning och övning skapar förutsättningar för det.

Olika uppgifter i organisationen förutsätter olika kunskap och kompetens rörande informationssäkerhet. Det är av vikt att utbildningen anpassas till både arbetsuppgifterna och den befintliga kompetensnivån i organisationen.

Myndigheten bör ha rutiner för utbildning som säkerställer att personalen har tillräcklig kunskap om gällande regler för informationssäkerhet. Rutinerna bör omfatta all personal.

Myndigheten bör ha en plan som säkerställer att all personal har tillräcklig kompetens för att kunna utföra sina arbetsuppgifter. Utbildning bör genomföras minst vartannat år.

Vid anlitande av externa parter bör krav ställas på tillräcklig kompetens avseende informationssäkerhet.

Övningar av myndighetens säkerhetsåtgärder för kontinuitetshantering avseende informationssäkerhet bör ske minst vartannat år. De bör utvärderas och erfarenheterna bör återkopplas till verksamheten.

Kommentarer till 9 §

Myndighetens systematiska informationssäkerhetsarbete bör ständigt utvecklas för att omhänderta interna och externa krav. Ett sådant arbete förutsätter flera steg som bygger på varandra och som sedan upprepas. Arbetet underlättas genom att myndigheten i förväg specificerar olika skyddsnivåer. Information med olika skyddsbehov kan därefter knytas till lämplig skyddsnivå. Med skyddsnivå menas grupperingar av åtgärder vilka används för att skydda information som med hjälp av informationsklassning konstaterats ha samma skyddsbehov.

Myndigheten bör kontinuerligt analysera hot och risker i verksamheten. Resultatet av genomförda analyser bör leda till beslut om anpassade säkerhetsåtgärder. Behovet av att säkerställa spårbarhet i informationshanteringen bör särskilt beaktas vid valet av säkerhetsåtgärder.

Myndigheten bör utveckla standardiserade skyddsnivåer där säkerhetsåtgärder sammanförs på ett sätt som motsvarar myndighetens informationsklassningsmodell.

Särskild uppmärksamhet bör läggas på att verksamhetens säkerhetskrav beaktas vid utveckling, upphandling, anskaffning och avveckling av resurser för informationsbehandling. Vid utveckling av e-tjänster bör åtgärder vidtas för att säkerställa att medborgare och samverkande parter inte drabbas av skada. Etablerade säkerhetsåtgärder bör verifieras och godkännas av ansvarig för informationsbehandling i it-systemet innan driftsättning.

Relevans och nytta av vidtagna åtgärder bör utvärderas genom regelbunden granskning och uppföljning. Intern granskning bör kompletteras med oberoende extern granskning.

Fortlöpande dokumentation om klassning, riskanalyser och andra bedömningar bör sammanställas på ett sätt som underlättar utvärdering av informationssäkerhetsarbetet.

I dokumentationen bör även informationssäkerhetsaspekter beaktas avseende

- myndighetens interna informationshantering,
- myndighetens information som hanteras av extern part, och
- tjänster som myndigheten erbjuder andra aktörer inom e-förvaltning eller motsvarande.

Vägledning för informationsklassning finns på www.msb.se.

Kommentarer till 10 -11 §§

Rutiner för intern incidenthantering bör vara utformade så att de bidrar till att mildra effekter av, säkra bevisning om, dra lärdomar från och förhindra upprepande av incident, samt för att underlätta återgång till normal drift.

Rutiner för intern incidenthantering bör vara kommunicerade till berörd personal och berörda externa parter. Kännedom om rutinerna bör regelbundet följas upp.

Myndigheten bör säkerställa att det finns rutiner för att hantera incidenter som kan ha orsakats av brottsliga gärningar.

Rapportering av inträffade incidenter bör regelmässigt ske till den eller de befattningshavare som utsetts för att leda och samordna informations-säkerhetsarbetet.

För att kontinuerligt kunna anpassa informationssäkerhetsarbetet till verksamhetens behov och på detta sätt bedriva ett ändamålsenligt informationssäkerhetsarbete, krävs kunskap om risker och sårbarheter, exempelvis information om inträffade incidenter. I sådan dokumentation som i övrigt krävs enligt 7 § bör både uppgifter om eventuella brister i det systematiska informationssäkerhetsarbetet och allvarligare incidenter ingå.

Intern incidenthantering bidrar till att säkerställa att myndigheten har möjlighet att uppfylla kraven på obligatorisk it-incidentrapportering för statliga myndigheter enligt förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2016:2) om statliga myndigheters rapportering av it-incidenter.

För att kunna sätta samman en helhetsbild över inträffade incidenter och händelser i myndighetens it-system och för att säkerställa jämförbarhet mellan loggar bör myndigheten se till att alla system har en enhetlig tid.

Större störningar, avbrott och kriser kan orsaka stora problem för en organisations informationshantering. Det kan exempelvis handla om långvariga elavbrott, omfattande sjukdomsfrånvaro hos personalen, allvarliga virusangrepp eller dataintrång samt översvämningar i datorhallar.

Rutiner för kontinuitetshantering ger möjlighet för en organisation att förbereda sig inför och därmed enklare kunna hantera organisationens behov vid större störningar, avbrott och kriser. Stöd för kontinuitetshanteringsarbetet kan hämtas från genomförda riskanalyser vilka ger en bild av de typer av störningar, avbrott och kriser som särskilt bör beaktas. En god kännedom om vilka de viktigaste verksamheterna är, och vilka resurser som är nödvändiga för att upprätthålla dem, underlättar arbetet.

I rutiner för kontinuitetshantering bör roller med tillhörande ansvar och befogenheter definieras. Rutinerna bör även säkerställa att verksamheten kan bedrivas enligt den nivå av kontinuitet som behöver upprätthållas och som beslutats.

Genom rutiner för kontinuitetshantering bör myndigheten efter genomförd analys av risker och sårbarheter

- säkerställa den nivå av kontinuitet för informationshantering som krävs vid större störningar, avbrott och kriser,
- identifiera alternativa arbetssätt,
- fastställa krisorganisation, samt
- fastställa hur stöd för återgång till normal verksamhet ska utformas.

Myndighetens rutiner rörande kontinuitetshantering bör regelbundet följas upp och utvärderas. Detta bör särskilt ske i samband med

- övningar där säkerhetsåtgärderna för kontinuitetshantering prövas, samt
- större organisationsändringar och förändrade verksamhetskrav.

Beställningsadress:
Wolters Kluwers kundservice, 106 47 Stockholm
Telefon: 08-598 191 90, www.wolterskluwer.se
E-post: kundservice@wolterskluwer.se