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 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter;

beslutade den xx mars 2020.

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

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

Begreppsförklaring

3 § I denna författning avses med

extern aktör	underleverantörer, inhyrda konsulter eller motsvarande.
informationssystem	applikationer, tjänster eller andra komponenter som hanterar information. I begreppet ingår också nätverk och infrastruktur.
informationssäkerhet	bevarande av konfidentialitet, riktighet och tillgänglighet hos information.
ledningssystem för informationssäkerhet	del av myndighetens övergripande ledningssystem, baserad på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och utveckla organisationens informationssäkerhet.

Utkontraktering

4 § Ansvaret som statliga myndigheter har för säker informationshantering i 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap gäller även när myndighetens information hanteras av en extern aktör.

5 § Myndigheten ska, innan den låter en extern aktör hantera information, identifiera och hantera riskerna en sådan hantering innebär. De säkerhetsåtgärder som den externa aktören ska vidta ska regleras i avtal och följas upp.

6 § I de fall en myndighet anlitar en annan myndighet för att fullgöra uppgifter som regleras i denna författning ska de berörda myndigheterna tydliggöra detta i en överenskommelse samt bedöma och hantera risker med myndigheternas samverkan. Ansvaret för informationsklassning enligt 10§ p.1 kan inte överlåtas.

Utformning av systematiskt och riskbaserat informationssäkerhetsarbete

Standarder, ansvar, resurser och integrering

7 § Varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet eller motsvarande.

8 § Det systematiska och riskbaserade informationssäkerhetsarbetet ska utformas utifrån de risker och behov myndigheten identifierar. Det ska omfatta all hantering av information som myndigheten ansvarar för. I utformningen av informationssäkerhetsarbetet ingår att myndigheten ska

1. tydliggöra myndighetsledningens och den övriga organisationens ansvar avseende informationssäkerhetsarbetet,
2. fördela de resurser och befogenheter som arbetet med informationssäkerhet kräver, detta gäller särskilt för den eller de som utses att leda och samordna arbetet,
3. integrera informationssäkerhetsarbetet med myndighetens befintliga sätt att leda och styra sin organisation, samt
4. säkerställa att myndighetens interna regler, arbetssätt och stöd för informationssäkerhetsarbete regelbundet och vid behov utvärderas och anpassas.

Utformningen av informationssäkerhetsarbetet ska dokumenteras.

Interna regler, policy och stöd

9 § Myndigheten ska säkerställa att det finns en informationssäkerhetspolicy där ledningens målsättning med och inriktning

för informationssäkerhetsarbetet framgår. Myndigheten ska också upprätta de interna regler och tillhandahålla det stöd som i övrigt krävs för informationssäkerhetsarbetet.

Systematiskt och riskbaserat informationssäkerhetsarbete

10 § Myndigheten ska ha ett dokumenterat arbetssätt för sitt informationssäkerhetsarbete som stöd för att

1. klassa 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 myndighetens information och informationssystem (riskbedömning),
3. utifrån genomförd informationsklassning och riskbedömning införa ändamålsenliga och proportionella säkerhetsåtgärder, samt
4. följa upp och utvärdera vidtagna säkerhetsåtgärder i syfte att vid behov anpassa skyddet av informationen och informationssystemen.

Myndigheten ska fortlöpande dokumentera vidtagna åtgärder enligt punkt 1- 4.

Kunskap och kompetens

11 § Myndigheten ska ha ett dokumenterat arbetssätt som säkerställer att medarbetarna har kunskap om säker hantering av information. I arbetet ingår att

1. hålla medarbetarna informerade om relevanta interna regler och stöd,
2. regelbundet och utifrån identifierat behov och medarbetarens arbetsuppgifter utveckla och upprätthålla medarbetarnas kompetens avseende informationssäkerhet genom utbildning, informationsinsatser och övning, samt
3. följa upp och utvärdera att interna regler, arbetssätt och stöd tillämpas på avsett sätt.

Hantering av incidenter och kontinuitet

12 § Myndigheten ska ha ett dokumenterat arbetssätt för att upptäcka, bedöma och vidta åtgärder för att minimera konsekvenserna av incidenter och avvikelser avseende myndighetens informationshantering. I arbetet ingår att säkerställa förmåga att

1. rapportera incidenter externt,
2. identifiera grundorsaker, samt
3. vidta åtgärder för att förhindra att liknande incidenter och avvikelser inträffar på nytt.

13 § Myndigheten ska ha ett dokumenterat arbetssätt för kontinuitetshantering som tydliggör hur

1. myndigheten ska identifiera behovet av kontinuitet vid incidenter och samhällsstörningar för informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag, samt
2. förmågan att upprätthålla identifierat behov av kontinuitet ska säkerställas och övas.

Fysiskt skydd och personalsäkerhet

14 § Myndigheten ska utifrån informationsklassning och riskbedömning vidta säkerhetsåtgärder som försvårar obehörigt tillträde till myndighetens lokaler där information hanteras. Det ska, där det inte är uppenbart onödigt, finnas tekniska system för att larma vid obehörigt tillträde till sådana lokaler.

15 § Myndigheten ska, om det inte är uppenbart onödigt, dela in sina lokaler där information hanteras i fysiskt separerade zoner. Behovet av zoner ska identifieras utifrån informationsklassning och riskbedömning. Behovet av särskilda besökszoner ska identifieras och hanteras.

16 § Myndigheten ska ha ett dokumenterat arbetssätt för att vid anställning och förändring av arbetsuppgifter anpassa bakgrundskontroller utifrån vilken information som medarbetaren ska få åtkomst till.

Uppföljning av informationssäkerheten

17 § Myndigheten ska som ett led i sitt uppföljningsarbete minst en gång per år sammanställa

1. resultatet av genomförda utvärderingar av interna regler och arbetssätt enligt 8 § p. 4,
2. resultatet av genomförda utvärderingar av att interna regler, arbetssätt och stöd tillämpas på avsett sätt enligt 11 § p. 3,
3. skillnaden mellan införda säkerhetsåtgärder och säkerhetsåtgärder specificerade i standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet eller motsvarande,
4. genomförda informationsklassningar enligt 10 § p. 1 och riskbedömningar enligt 10 § p. 2, samt
5. utvärderingar av ändamålsenligheten av vidtagna säkerhetsåtgärder enligt 10 § p. 4.

18 § Myndighetens ledning ska i sin löpande bedömning av om myndighetens information hanteras på ett säkert och effektivt sätt, minst informera sig om

1. resultatet av genomförda utvärderingar enligt 8 § p. 4 och 11 § p. 3 som avser myndighetens arbetssätt för att identifiera, analysera och värdera risker i myndighetens informationshantering,
2. i vilken utsträckning vidtagna säkerhetsåtgärder motsvarar identifierat behov,
3. kvarvarande risker i myndighetens informationshantering utifrån allvarlighetsgrad, samt
4. identifierade hinder för att uppnå ledningens målsättning med och inriktning för informationssäkerhetsarbetet inklusive identifierade brister avseende tilldelning av ansvar, resurser, mandat och befogenheter.

Denna författning träder i kraft den 1 juli 2020. Samtidigt upphör Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2016:1) om statliga myndigheters informationssäkerhet att gälla.