Myndigheten för samhällsskydd och beredskaps författningssamling

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

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

Förslag till
Allmänna råd om informationssäkerhet för statliga myndigheter;

beslutade den xx mars 2020.

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.

Utkontraktering

5 § I avtalet mellan myndigheten och den externa aktören bör regleras hur uppföljning av överenskomna säkerhetsåtgärder och det systematiska och riskbaserade informationssäkerhetsarbetet ska ske. Dessutom bör det framgå hur den externa aktören ska överlämna information till myndigheten om misstänkta eller inträffade incidenter, avvikelser och sårbarheter. Avtalet bör även specificera hur myndighetens information ska återhämtas när avtalet upphör. Krav på att den externa aktören har tillräcklig kunskap och kompetens avseende informationssäkerhet bör också ingå i avtalet.

Utformning av systematiskt och riskbaserat informationssäkerhetsarbete

Standarder, ansvar, resurser och integrering

7 § Om en myndighet väljer att använda en annan standard än de som anges i 7 § i denna författning bör myndigheten analysera och dokumentera de likheter och skillnader som finns mellan respektive standarder. Analysen bör ge underlag för att säkerställa att vald standard ger tillräckligt stöd i arbetet.

8 § En myndighet bör minst en gång per år utvärdera hur interna regler, arbetssätt och stöd svarar mot identifierade risker och behov. Utvärdering bör också ske i samband med verksamhetsuppföljning, omorganisationer, förändrade rättsliga krav, förändringar rörande informationssystem samt vid hantering av extern aktör.

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

Systematiskt och riskbaserat informationssäkerhetsarbete

10 § Av det dokumenterade arbetssättet för informationsklassning och riskbedömning bör framgå

- kriterier och nivåer för bedömning av konsekvens som bedömningarna ska ske enligt,
- när och i vilka situationer informationsklassning och riskbedömning ska genomföras, samt
- vilken funktion som ansvarar för att informationsklassning och riskbedömning genomförs.

Vid bedömning av risker bör även hot och sårbarheter identifieras och värderas.

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.

Myndigheten bör särskilt bedöma vilka risker som kan uppkomma i informationssystem när information ackumuleras eller aggregeras.

Vid val av ändamålsenliga och proportionella säkerhetsåtgärder bör myndigheten kombinera organisatoriska, administrativa, fysiska och tekniska åtgärder. Myndighetens behov av spårbarhet samt äkthet och ursprung (autenticitet) hos informationen bör särskilt beaktas.

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.

Kunskap och kompetens

11 § Arbetssättet bör säkerställa att medarbetare med särskilt utpekade funktioner i informationssäkerhetsarbetet har tillräcklig kunskap och kompetens om säker informationshantering för att kunna utföra sina arbetsuppgifter.

Hantering av incidenter och kontinuitet

12 § Inträffade incidenter och avvikelser bör föranleda översyn av det systematiska och riskbaserade arbetssättet samt införda säkerhetsåtgärder.

I syfte att utveckla skyddet av information och informationssystem bör den eller de som utsetts att leda och samordna informationssäkerhetsarbetet hos myndigheten ha åtkomst till information om inträffade incidenter och avvikelser.

13 § Av arbetssättet för att uppnå kontinuitet för myndighetens informationshantering bör följande framgå

- hur tillgänglighetskraven från genomförd informationsklassning omhändertas i kontinuitetsarbetet,
- vilka kriterier som ska användas för att bestämma accepterad återställandetid för informationssystem,
- hur beslut om att tillämpa alternativa arbetssätt respektive beslut om att återgå till normalt arbetssätt fattas, samt
- vilka kriterier som ska användas för att identifiera myndighetens behov av uthållighet över tid.

Utvärdering av kontinuitetsarbetet bör särskilt ske efter genomförda övningar, vid organisationsförändringar inklusive när information överlämnas till extern aktör. Detsamma gäller vid förändrade rättliga krav eller verksamhetskrav, samt om brister upptäcks i samband med att alternativa arbetssätt används.

Uppföljning av informationssäkerheten

14 § I de fall myndigheten har identifierat ytterligare krav på säkerhetsåtgärder som går utöver standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet eller motsvarande bör även skillnaden mellan dessa ytterligare krav och införda säkerhetsåtgärder sammanställas.