Svar på remiss gällande förslag till: Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter

Svarande organisation: Skatteverket, diarienummer: 202 525319-19/112

Referens/diarienr: 2019-14545

Om Excelarket
Genom att klicka på "välj" får du upp en för kolumnen anpassad rullista
Välj "övrigt" där inget annat alternativ är lämpligt.
Synpunkter på konsekvensutredningen lämnas från rad 115.

Synpunkter föreskrifter

§	Punkt	Synpunkter	Förslag till ändring	Övriga kommentarer
1	Välj	För den ovane läsaren kan det vara otydligt vilken informationshantering och vilka myndigheter som omfattas av denna föreskrift. Därför föreslår Skatteverket ett tillägg här.	1 § Denna författning innehåller bestämmelser om sådana säkerhetskrav som avses i 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. **Bestämmelserna avser grundläggande och särskilda säkerhetskrav för att myndigheters verksamhet ska kunna utföras på ett tillfredsställande sätt. Bestämmelserna gäller för samtliga statliga myndigheter under regeringen.**	Förtydliga att det gäller statliga myndigheter samt både grundläggande och särskilda säkerhetskrav för en tillfredsställande verksamhet i vardag, kris och höjd beredskap.
3	Välj	I det allmänna rådet bör det finnas en hänvisning till SIS-TR 50:2015. Överväg att förklara ytterligare begrepp som används i förordningen exempelvis informationsklassning, riskbedömning mfl.		Begrepp och definitioner skiljer sig jämfört med andra regleringar inom säkerhetsområdet, tex säkerhetsskyddsregleringen, dataskyddsregleringen. Det kan medföra svårigheter att tolka bestämmelser och genomföra åtgärder.
4	Välj	Myndigheter använder utöver externa aktörer även andra myndigheter för informationshantering.	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 **eller annan myndighet.**	
5	Välj	I det allmänna rådet 5 § bör det finnas en hänvisning till att risker bör hanteras enligt SS-ISO/IEC 27005:2018		Synpunkten berör Allmänna råd 5 § Utkontraktering
6	Välj	En utförande myndighet kan behöva hantera mycket stora informationsmängder från olika myndigheter. Skatteverket föreslår att lägga till ett allmänt råd, till 6 §, angående den utförande myndighetens ansvar för informationsklassificering.		Allmänna råd: Det kan förekomma att den utförande myndigheten kan behöva tillämpa en högre informationsklassificering pga ackumelerade och aggregerade informationsmängder.
8	Välj	I det allmänna rådet 8 § bör myndighetens behov vara avgörande för hur ofta utvärdering ska ske.		Allmänna råd: 8 § En myndighet bör **regelbundet** utvärdera hur interna regler, arbetssätt och stöd svarar mot identifierade risker och behov. Utvärdering **bör 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.

9	Välj	Föreskrifterna bör möjliggöra ett integrerat säkerhetsarbete. Skatteverket föreslår därför en formulering som gör det möjligt att ha en säkerhetspolicy där informationssäkerhet ingår.	9 § Myndigheten ska säkerställa att det finns en **policy** 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.	
10	1	Klassning av konfidentialitet, riktighet och tillgänglighet behöver genomföras utifrån sitt verksamhets- och systemsammanhang. Skatteverket föreslår att det förtydligas genom ett tillägg i det allmänna rådet 10 § Systematiskt och riskbaserat informationssäkerhetsarbete.		Exempelvis kan en personuppgift i ett sammanhang ha tillgänglighetskrav på millisekunder och i ett annat sammanhang ha krav på svar inom en månad. Allmänna råd: **Informationen bör klassas i sitt sammanhang där den specifika informationen hanteras.**
11	Välj	Kunskapsutveckling inom en organisation är både komplext och varierade och bör inte detaljregleras i en föreskrift. Det kan misstolkas som att MSB går utanför sitt bemyndigande. Skatteverket föreslår att i det allmänna rådet 11 § skulle kunna innehålla detaljerna från föreskriften 11 §.	11§ Myndigheten ska ha ett dokumenterat arbetssätt som säkerställer att medarbetarna **inom ramen för sina arbetsuppgifter** har **tillräcklig** kunskap om **informationssäkerhet, gällande regler och interna rutiner över tid.**	Allmänna råd: **Myndigheten bör integrera informationssäkerhet i sitt ordinarie arbetssätt för medarbetarutveckling. I arbetssättet bör ingå 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.
12	Välj	Bör överväga om inte föreskriften MSBFS 2016:2 föreskrifter och allmänna råd om statliga myndigheters rapportering av it-incidenter ska ingå i samma föreskrift. Skatteverket menar att incidentrapporteringen utgör en grund för att kontinuerligt utveckla informationssäkerhetsarbetet genom ständiga förbättringar. Detta bör framgå av det allmänna rådet.		Allmänna råd: 12 § Inträffade incidenter och avvikelser bör ingå i arbetssättet för att ständigt förbättra myndighetens informationssäkerhetsarbete.
15	Välj	Sista meningen i 15 §, "Behovet av särskilda besökszoner ska identifieras och hanteras." , är onödig då det redan framgår av det generella kravet i den andra meningen. Meningen kan också misstolkas som att MSB går utanför sitt bemyndigande utifrån krisberedskapsförordningen. Skatteverket föreslår att sista meningen flyttas till allmänna råd.	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.**	Allmänna råd: Behovet av särskilda besökszoner **bör** identifieras och hanteras.

17	3	Det som efterfrågas i punkt 3 är en mycket omfattande arbetsinsats där hela verksamhetens informationshantering ska jämföras mot två mycket omfattande internationella standarder, ISO 27001 och 27002. De övriga punkterna beskriver sammanställning av under året genomfört säkerhetsarbete. Skatteverket föreslår att 17 § p3 bryts ut till en egen paragraf. En GAP mot hela ISO 27001 och 27002 för all informationshanteirng är inte ändamålsenlig eller proportionell att genomföra från grunden varje år. Med en egen paragraf är det fortfarande en mycket stor arbetsinsatts men den behöver inte göras från grunden varje år.	**17a §** Myndigheten ska som ett led i sitt **systematiska informationssäkerhetsarbete sammanställa** 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. 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. genomförda informationsklassningar enligt 10 § p. 1 och riskbedömningar enligt 10 § p. 2, samt 4. utvärderingar av ändamålsenligheten av vidtagna säkerhetsåtgärder enligt 10 § p. 4.	
18	Välj	Texten är detaljerad och kan ge intryck av att informationen till ledningen ska vara omfattande och detaljerad. Det är inte alltid en myndighetsledning vill ha den typen av detaljerad information. Utmaningen är att formulera rapporteringen på ett kortfattat och begripligt sätt. Därför föreslår Skatteverket att MSB i allmänna råd tar fram exempel på hur det kan utformas på ett pedagogiskt sätt.		Ge gärna exempel i allmänna råd på hur man på ett allmänt och begripligt sätt håller sin ledning uppdaterade med förslag till metodstöd.
Välj	Välj			

Behöver du fler rader att lämna synpunkter på:
Infoga så många rader du behöver. Du kan behöva kopiera listan.

Synpunkter Konsekvensutredningen		
Rubrik	**Synpunkter**	**Övriga kommentarer**