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

Svarande organisation:	**Skatteverket, diarienummer: 202 525319-19/112**
Referens/diarienr:	**2019-14546**

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

Kap	§	Punkt	Synpunkter	Förslag till ändring	Övriga kommentarer
1	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 systemadministrativ behörighet.		Begrepp och definitioner skiljer sig jämfört med andra regleringar inom säkerhetsområdet, tex säkerhetsskyddsregleringen, dataskyddsregleringen. Det kan medföra svårigheter att tolka bestämmelser och genomföra åtgärder.
2	2	Välj	Kravet på en ansvarig per informationssystem kan uppfattas som alltför detaljstyrande med tanke på myndigheternas skiftande it-miljöer och förutsättningar i övrigt. Därför föreslås en mer generell skrivning.	2 kap. 2 § Myndigheten **ska för informationssystem ha en dokumenterad ansvarsfördelning** som ska säkerställa att ändamålsenliga och proportionella säkerhetsåtgärder införs, förvaltas, följs upp och utvärderas.	
2	3	Välj	Den föreslagna bestämmelsen är för detaljerad. Den är inte rimlig och kostnadseffektiv jämfört med risk kontra nytta för alla myndigheter. Bestämmelsen bör utgå eller omformuleras så att det ger myndigheterna större möjlighet att styra nivå av inventering för informationssystem. En myndighet har ofta flera informationssystem där bestämmelsen inte är motiverad. För mer skyddsvärda informationssystem ska det finnas en förteckning men det bör vara upp till myndigheterna själva att bestämma detta i sitt systematiska och riskbaserade informationssäkerhetsarbete.		
2	4	Välj	Kravet på kompetensbeskrivning per informationssystem uppfattas som alltför detaljstyrande med tanke på myndigheternas skiftande it-miljöer och förutsättningar i övrigt. Skatteverket anser att bestämmelsen bör omformuleras så att den kan tillämpas på alla myndigheter och typer av it-miljöer.	2 kap. 4 § Myndigheten **ska dokumentera** vilka kompetenser och resurser som krävs för att upprätthålla säkerheten över tid.	
2	5	Välj	Överväg om bestämmelsen behövs med hänsyn till att det redan regleras i 10 § infosäk-föreskriften.		
3	4	Välj	Kraven är för detaljerade och inte anpassade till myndigheternas skiftande behov och förutsättningar. Skatteverket anser att bestämmelsen bör omformuleras så att den kan tillämpas på alla myndigheter och typer av it-miljöer. Skatteverket föreslår att detaljer beskrivs i allmänna råd.	3 kap. 4 § Myndigheten ska innan driftsättning och inför förändring som kan påverka säkerheten i informationssystem kontrollera att ställda krav på säkerhet **uppfylls.** I de fall säkerhetsbrister kvarstår ska dessa riskbedömas och hanteras innan driftsättning eller förändring.	Allmänna råd: Kontroll före driftsättning bör ske genom säkerhetstester och granskning.

3	5	Välj	Kraven är för detaljerade och inte anpassade till myndigheternas skiftande behov och förutsättningar. Skatteverket anser att bestämmelsen bör omformuleras så att den kan tillämpas på alla myndigheter och typer av it-miljöer. Skatteverket föreslår att detaljer beskrivs i allmänna råd.	3 kap 5 § Myndigheten ska innan driftsättning och inför förändring kontrollera att det för berört informationssystem finns korrekt och tillräcklig dokumentation **som stöd för strukturerad och säker drift samt förvaltning.**	Allmänna råd: Dokumentationen bör minst omfatta arkitektur, ingående komponenter, konfiguration, dataflöden och övrig relevant systeminformation.
4	1	Välj	Kraven är för detaljerade och inte anpassade till myndigheternas skiftande behov och förutsättningar. Skatteverket anser att bestämmelsen bör omformuleras så att den kan tillämpas på alla myndigheter och typer av it-miljöer. Det bör vara upp till respektive myndighet att i sitt systematiska och riskbaserade informationssäkerhetsarbete avgöra sitt behov av separation. Skatteverket föreslår att detaljer beskrivs i allmänna råd.	4kap. § 1 Myndigheten ska **analysera sina IT-komponenter och dokumentera behovet av placering i separata nätverkssegment för att förhindra spridning av it-incidenter.**	Allmänna råd: För att förhindra spridning av it-incidenter **bör** om det inte är uppenbart onödigt, följande placeras i separata nätverkssegment 1. klienter för användare, 2. klienter för administration, 3. servrar, 4. centrala systemsäkerhetsfunktioner i form av behörighetskontrollsystem, säkerhetsloggning, filtrering och liknande, 5. centrala stödfunktioner i form av skrivare, scanner och liknande, 6. trådlösa nätverk, 7. gästnätverk, 8. externt åtkomliga tjänster, 9. informationssystem som sammankopplas med extern leverantör, 10. industriella informations-och styrsystem, samt 11. system som innehåller sårbarheter som inte kan hanteras.
4	2	Välj	Den föreslagna bestämmelsen är för detaljerad och inte kostnadseffektiv för de flesta myndigheter. Skatteverket föreslår att bestämmelsen utgår eller blir ett allmänt råd.		
4	3	Välj	Bestämmelsen är för detaljstyrd och bör i större grad vara upp till myndigheterna själva att avgöra i sitt systematiska och riskbaserade informationssäkerhetsarbete. Syftet med unika identiteter försvinner lite om man inte samtidigt ställer krav på att de också ska vara unika över tid.	4 kap. 3 § Myndigheten ska, **om det inte är uppenbart olämpligt,** säkerställa att samtliga identiteter i myndighetens produktionsmiljö **är unika över tid.** Alla identiteter ska innan de kopplas till en individ eller ett informationssystem godkännas och dokumenteras.	Med uppenbart olämpligt menar Skatteverket att ett exempel kan vara om polisen/SÄPO har konton som de använder för åtkomst till ett informationssystem hos en annan myndighet där den andra myndigheten inte vill registrera utomstående personers identiteter i myndighetens behörighetsdatabas.
4	4	Välj	Bestämmelsen bedöms inte vara proportionell eller ändamålsenlig då säkerhetsvinsten är liten och kostnaden för att skapa och följa upp trippla identiteter blir orimligt stora. Myndigheten måste själv avgöra detta i sitt systematiska och riskbaserade arbete.		
4	5	Välj	Inom stora myndigheter behöver denna översyn ske på rollnivå i högre utsträckning än på individnivå. Godkännanden sker på individnivå men tilldelningen behöver av praktiska skäl hanteras på roll-nivå.	4 kap. 5 § Myndigheten ska utforma sin behörighetshantering på ett sådant sätt att varje identitet **eller roll** inte har mer åtkomst till information än vad arbetsuppgiften kräver.	
4	6	Välj	Kraven är för detaljerade och inte anpassade till myndigheternas skiftande behov och förutsättningar. Skatteverket anser att bestämmelsen bör omformuleras så att den kan tillämpas på alla myndigheter och typer av it-miljöer samt föreslår att sista meningen i bestämmelsen flyttas över till ett allmänt råd.	4 kap. 6 § Identiteter som ger systemadministrativ behörighet får endast användas för systemadministration och ska tilldelas **restriktivt.**	Allmänna råd: En identitet med systemadministrativ behörighet **bör** endast ges åtkomst till en begränsad del av produktionsmiljön.

4	7	Välj			Behörighetsstyrningen bör vara en del av det systematiska och riskbaserade informationssäkerhetsarbetet.
4	8	Välj	Kraven är för detaljerade och inte anpassade till myndigheternas skiftande behov och förutsättningar. Skatteverket anser att bestämmelsen bör omformuleras så att den kan tillämpas på alla myndigheter och typer av it-miljöer. Sista meningen bör utgå eller möjligen flyttas till allmänt råd.	4 kap. 8 § Myndigheten ska identifiera och hantera behov av separata katalogtjänster för **behörigheter.**	
4	9	Välj	Kraven är för detaljerade och inte anpassade till myndigheternas skiftande behov och förutsättningar. Skatteverket anser att bestämmelsen bör omformuleras så att den kan tillämpas på alla myndigheter och typer av it-miljöer. Det bör vara upp till respektive myndighet att i sitt systematiska och riskbaserade informationssäkerhetsarbete avgöra behovet av flerfaktorsautentisering.	4 kap. 9 § Flerfaktorsautentisering ska användas, **om det inte är uppenbart onödigt,** vid 1. åtkomst till produktionsmiljön via externt nätverk, 2. systemadministrativ åtkomst, samt 3. åtkomst till informationssystem som hanterar uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400).	
4	11	Välj			Alternativ till komplexa lösenord kan vara långa lösenordsfraser. Allmänna råd Myndigheten bör ha interna regler för antalet tillåtna försök, tidslängd för låsning och krav på administrativt återställande.
4	12	Välj	4 kap. 12 och 13 §§ bör övervägas om de kan slås ihop då de i princip säger samma sak.		
4	13	Välj	4 kap. 13§ se synpunkt 4 kap. §12		
4	14	Välj	Kravet är inte kostnadseffektivt jämfört med risk kontra nytta och effektivitet. Speciellt inte att kryptera en myndighets alla säkerhetsloggar för alla informationssystem. Bör vara upp till myndigheterna själva att avgöra i sitt systematiska och riskbaserade informationssäkerhetsarbete.	4 kap. 14 § Myndigheten ska, **om det inte är uppenbart olämpligt,** använda kryptering för att skydda säkerhetsloggar, lösenord och koder mot **obehörig förändring och åtkomst** vid kommunikation och lagring.	
4	15	Välj	Det finns flera situationer där kraven inte är uppenbart onödigt men ändå olämpligt eller inte rekommenderat. Bestämmelsen bör omformuleras enligt förslag.	4 kap. 15 § Myndigheten ska, om det inte är uppenbart onödigt **eller olämpligt,** införa 1. elektronisk signering och kryptering av e-post, 2. verifiering av signerad e-post, och 3. Domain Name System Security Extensions (DNSSEC).	
4	16	Välj	Kraven är för detaljerade och inte anpassade till myndigheternas skiftande behov och förutsättningar. Säkerhetskonfigureringen kan även genomföras av extern aktör. Skatteverket anser att bestämmelsen bör omformuleras så att den kan tillämpas på alla myndigheter och typer av it-miljöer.	4 kap. 16 § Innan informationssystem tas i drift ska **säkerhetskonfigurering genomföras, dvs kontroll av att funktioner som inte behövs stängs av eller tas bort, byta ut förinställda lösenord samt anpassning av** förinställda konfigurationer till identifierat behov av funktionalitet och säkerhet.	
4	18	Välj	Kraven är för detaljerade och inte anpassade till myndigheternas skiftande behov och förutsättningar. Begreppet programvara uppfattas som otydligt. Skatteverket anser att bestämmelsen bör omformuleras så att den kan tillämpas på alla myndigheter och typer av it-miljöer.	4 kap. 18 § Myndigheten ska **ha interna regler för installation av programkod som exekveras** i myndighetens produktionsmiljö.	Allmänna råd Myndigheten bör säkerställa att endast individer med systemadministrativa behörigheter kan installera programkod som exekveras i myndighetens produktionsmiljö.

4	20	Välj		4 kap. 20 § Myndigheten ska utan onödigt dröjsmål byta ut programvaror som inte längre uppdateras av leverantören. **Föreligger det hinder för utbyte ska risker med att använda programvara som inte längre uppdateras av leverantören riskbedömas.**	Endast språklig komplettering i andra meningen.
4	22	Välj			Flera andra alternativ finns som uppfyller syftet.
4	23	Välj	Förtydliga att det endast ska omfatta myndigheternas egen information, inte all information som behövs för myndighetens förmåga att utföra sitt uppdrag, då det innebär att myndigheter behöver säkerhetskopiera andra parters information också.	4 kap. 23§ Myndigheten ska säkerhetskopiera information **hos myndigheten** som behövs för myndighetens förmåga att utföra sitt uppdrag minst en gång per dygn.	
4	26	Välj	Kraven är för detaljerade och inte anpassade till myndigheternas skiftande behov och förutsättningar. Skatteverket anser att bestämmelsen bör omformuleras så att den kan tillämpas på alla myndigheter och typer av it-miljöer. Detaljer kan utgöra allmänna råd annars är risken att sekretess kommer att skymma andra krav på spårbarhet exempelvis riktighetskrav.	4 kap. 26 § Myndigheten ska dokumentera vilka uppgifter som ska loggas och var loggningsuppgifter ska hämtas. Säkerhetsloggningen ska skapa spårbarhet och **logga händelser som kan påverka säkerheten i informationssystem som har betydelse för myndighetens verksamhet.**	Allmänna råd: Säkerhetsloggningen bör minst omfatta 1. användares och systemadministratörers åtkomst till uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), 2. systemadministratörers förändringar av konfigurationer och systemsäkerhetsfunktioner, samt 3. förändringar i åtkomsträttigheter.
4	31	Välj	Det finns många olika informationssystem och många alternativa sätt att skydda sig mot skadlig kod. Att ställa krav på just programvara för detta medför inte tillräcklig säkerhetsnytta baserat på risk och effektivitet. Bestämmelsen bör omformuleras där fler alternativ för skydd mot skadlig kod tillåts.	4 kap. 31 § Myndigheten ska skydda nätverksanslutna **informationssystem mot** skadlig kod.	
4	32	Välj	Det är otydligt vad som avses med it-utrymme och särskilt it-utrymme.		Överväg behovet av allmänna råd avseende särskilda it-utrymmen och it-utrymmen relativt tidigare vägledning från MSB.
4	33	Välj	Kraven är för detaljerade och inte anpassade till myndigheternas skiftande behov och förutsättningar. Skatteverket anser att bestämmelsen bör omformuleras så att den kan tillämpas på alla myndigheter och typer av it-miljöer. Det är inte alltid motiverat att tillträdesdokumentation måste sparas 5 år.	4 kap. 33 § Myndighetens särskilda it-utrymmen ska skyddas mot obehörig åtkomst genom tillräckligt skalskydd. Tillträde till särskilda it-utrymmen ska registreras på **individnivå.**	Överväg att ha detaljkraven om tidsperspektivet i allmänna råd.
5	2	Välj	Otydligt vad som avses med bestämmelsen.		
Välj	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**
Uppgifter om vilka kostnadsmässiga och andra konsekvenser regleringen medför och en jämförelse av konsekvenserna för de övervägda regleringsalternativen	Skatteverket saknar resonemanget kring myndigheternas kompetensförsörjning gällande informationssäkerhet och it-säkerhet. Kompetensförsörjningen är en kritisk förutsättning om dessa föreskrifter ska kunna tillämpas.	Konsekvensutredningarna bör kompletteras med uppskattningar för ökade kostnader för medarbetare, utbildning och övergripande förvaltningskostnader. Kostnader för hård- och mjukvara är vanligtvis för en myndighet en liten kostnad jämfört med övrig löpande förvaltning av säkerhetsarbetet. Kostnad för alla it-säkerhetskrav behöver sättas i relation till vilken uppskattad förbättring av myndighetens informationssäkerhet som it-säkerhetskravet medför.