Svar på remiss gällande förslag till: **Föreskrifter och allmänna råd om säkerehtsåtgärder och utbildning, Diarienummer MSB 2025-13269**

Svarande organisation: **Stiftelsen för Internetinfrastruktur**

Intern referens: **Legal, Regulatory, Compliance**

Synpunkter föreskrifter och allmänna råd					
Kapitel	**§**	**Punkt**	**Synpunkt**	**Förslag till ändring**	**Kommentar**
kap. 1	3		Saknas detaljerade förklaring av "cybersäkerhetskris".		Uttryck vad som menas istället för att hänvisa till en artikel.
kap. 1	3		Säkerställ termer i MSB:s termbank.		Ta hjälp av SIS för termer.
kap. 1	3		Definiera "samordnare".		Definiera "samordnare" i MSB:s termbank.
kap. 1	3		Definiera "öva" och "test".	Övning - syftar till att träna, bedöma och förbättra organisationens prestation. Test - syftar till att erhålla ett godkänt eller icke godkänt resultat.	Definiera begreppen för att visa på skillnad mellan åtgärderna.
kap. 1	3		Definiera "kunskap" och "kompetens".		Gör en bedömning om det finns behov att förklara skillnad mellan begreppen.
kap. 1	3		Definiera "kris".		Gör en bedömning om det finns behov att definiera begreppet, i syfte att avgränsa dess betydelse. Det vill säga om det främst hänger ihop med sektorskritiskt system och/eller viktig samhällsfunktion.
kap. 2	1		Verksamhetsutövaren ska identifiera och hantera behovet av att använda relevanta standarder i arbetet - Bra.		Formuleringen ”Verksamhetsutövaren ska identifiera och hantera behovet av att använda relevanta standarder i arbetet” är i sig en förbättring jämfört med det tidigare förslaget ”bedriva … arbetet med stöd av relevanta standarder”, men grundproblemet kvarstår: antingen ger man verksamheterna utrymme att arbeta standardbaserat och verksamhetsanpassat, eller så detaljstyr man i föreskrift. Att försöka göra båda samtidigt skapar otydlighet, dubbelarbete och riskerar att sänka effektiviteten i säkerhetsarbetet. Vi vill samtidigt understryka att NIS2-direktivet och cybersäkerhetslagen i grunden är väl avvägda. Problemet ligger i den nivå av detaljstyrning som nu föreslås i MSB:s föreskrifter, inte i lagstiftningen som sådan.

kap. 2	3		Uppräkningen bör ändra följd, där det inleds med externa krav, interna behov och risker, alternativ att punkt 1 och 2 slås ihop.	1. Utformas utifrån externa krav, interna behov och risker. 2. Utgå från ledningens mål och inriktning 3. … 4. … Alternativt 1. utgå från externa krav, interna behov och risker för att stödja uppfyllnad av ledningens mål och inriktning .2 …	Uppräkningen bör hämta vägledning från ISO27001 kap 4. Först förstå organisationen och dess förutsättningar, förstå intressenters behov och förväntningar, omfattning för ledningssystemet. Därefter ledarskapets åtagande.
kap. 2	3		Paragraf 2 och 3 upprepar delvis kraven.	Se över möjligheten att slå ihop paragraferna.	Det skapar tydligare översikt med färre delvis överlappande paragrafer.
kap. 2	4		Bestämmelserna går djupt ned i organisations- och processnivå (vad dokumenten ska innehålla, hur de ska följas upp, hur beslut ska dokumenteras). Detta riskerar att bli oproportionerligt för mindre aktörer och går utöver vad som rimligen krävs för att uppfylla NIS2 och cybersäkerhetslagen.		Det finns en risk att MSB:s föreskrifter blir alltför detaljerade och riskerar att motverka sitt syfte under de närmaste åren. I stället för att stärka den faktiska säkerheten kommer många verksamheter sannolikt att lägga oproportionerligt mycket tid på att införa och förvalta administration, dokumentation och formalia.
kap. 2	4		Kraven på dokumentation av interna regler och arbetssätt ska bevaras i minst fem år. Här efterfrågar vi en tydlig motivering: Vad är den förväntade nyttan av just denna tidsfrist? På vilket sätt bidrar kravet till faktisk höjd cybersäkerhet, utöver redan befintliga krav på dokumenthantering och spårbarhet? Hur är det tänkt att mindre verksamheter praktiskt ska säkerställa detta, utan att administrativa bördor tränger undan annat viktigt säkerhetsarbete?		Vår uppfattning är att dokumentations- och bevarandekrav bör vara tydligt kopplade till risk och nytta, samt utformas så att de är proportionerliga för både stora och små verksamheter. I nuvarande form finns en betydande risk att tyngdpunkten hamnar på att producera och lagra dokument, snarare än på att utveckla och upprätthålla ett effektivt, riskbaserat säkerhetsarbete.
kap. 2	4		Ska det tolkas som att det är alla versioner som ska sparas i 5år? Eller endast senaste gällande?		
kap. 2	4		Flytta vissa detaljerade krav till allmänna råd och markera tydligare att omfattningen av dokumentation och formaliseringsgrad ska stå i proportion till verksamheten, dess omfattning och risk.		Skapar utrymme för små och medelstora aktörer att uppnå god cybersäkerhet utan orimlig administrativ börda, samtidigt som stora aktörer fortsatt kan ha omfattande dokumentation.
kap. 2	4	4	Punkt 4 och punkt 6 är delvis överlappande.	Se över möjligheten att slå ihop punkterna.	Det skapar tydligare översikt med färre delvis överlappande punkter.
kap. 2	4	6	Punkt 4 och punkt 6 är delvis överlappande.	Se över möjligheten att slå ihop punkterna.	Det skapar tydligare översikt med färre delvis överlappande punkter.
kap. 2	5		Paragrafen upprepar del av paragraf 4.	Se över möjligheten att slå ihop paragraferna.	Det skapar tydligare översikt med färre delvis överlappande paragrafer.
kap. 2	6	1	Tydliggör att ansvaret grundar sig på paragraf 2-3.		
kap. 2	6	2	Tydliggör att ansvaret grundar sig på paragraf 2-3.		
kap. 2	6	4	Se över behovet att sätta en minimumnivå på kompetens.		Se synpunkt ovan om att definiera "kompetens".
kap. 2	6	7	Det kan behövas vägledning från MSB för förståelse hur detta kan och bör göras.		
kap. 2	6	8	Det kan behövas vägledning från MSB för förståelse hur detta kan och bör göras.		

kap. 2	6	10	Se över behovet att avgränsa "säkerhetsåtgärder".	Hänvisning till paragraf 8.	Oklart om alla säkerhetsåtägrder avses, eller de som identifierats som väsentliga/kritiska i punkt 6-9.
kap. 2	8		”Minst årligen” kombinerat med en mycket omfattande lista över punkter kan bli tung administrativt, särskilt om organisationen redan har etablerade styr- och rapportstrukturer.	Tydliggör i allmänna råd att rapportering och övervakning kan integreras i befintliga ledningsstrukturer, och att frekvens och detaljeringsgrad kan anpassas efter risk, så länge kraven i sak uppfylls.	Ökar möjligheten att integrera cybersäkerhetsstyrningen i ordinarie ledningssystem, vilket stärker långsiktigheten.
kap. 2	8		Saknar skrivning om uppföljning av utförda övningar och tester.	Tillägg ny punkt 9: resultat av genomförd test av säkerhetsåtgärder.	
kap. 2	13-16		paragraf 13-16. Strukturen ligger nära standardpraxis (t.ex. ISO 27001/27005), men relationen till dessa standarder framgår inte tydligt och det finns risk för parallella system.	Hänvisa till ISO27005 Riskhantering för informationssäkerhet.	
kap. 2	16		Paragraf 16: Att följa upp säkerhetsåtgärder enligt åtgärdsplanen vid behov men minst var tredje månad är inte hållbart.	Vid behov eller årligen eller enligt organisationens riskacceptans.	
kap. 2	18		Paragraf 18: Varför inte hänvisa till ISO22301 för just kontinuitetshantering för att få fler att arbeta utifrån standarder.	Hänvisa till ISO22301 för kontinuitetshantering.	
kap. 2	24		Paragraf 24 vad menas med samordnare?	Definera rollen.	
kap. 3	4	1	Varför inte inkludera samordnaren i denna punkt från början med för att säkerställa att samordnare stöttar I säkerhetsarbetet från början tillsammans med informationsägare och systemägare	Informationsägare och systemägare tillsammans med samordnaren involveras i arbetet från start för att…	Denna ger tydligare riktning mot "security-by-design".
kap. 3	7		Kraven på dokumentation för arkitektur, system, hårdvara, mjukvara och risker är omfattande. För mindre och medelstora aktörer kan detta bli en tröskel, särskilt där IT-miljön redan är relativt enkel.	Förtydliga i allmänna råd att detaljeringsgraden kan skalas med hänsyn till komplexitet och risk till exempel att små, homogena miljöer kan dokumenteras mer översiktligt.	
kap. 3	22-24		Paragraf 22-24 Kraven på loggning är omfattande och kan leda till stora volymer personuppgifter. Förhållandet till dataskyddslagstiftning och gallring behandlas inte uttryckligen.	Komplettera allmänna råd med hänvisning till dataskyddsregler och behovet av proportionalitet i loggning och bevarandetider, ska motiveras av risk och rättsliga krav.	Bör kanske referera till MSBs riktlinjer kring att spara säkerhetsloggar i fem år.
kap. 3	26		Utvärdera om andra stycket "Säkerhetsloggarna ska utformas på ett sätt som möjliggör jämförbarhet mellan olika loggar. Loggarna ska vara tillgängliga för analys under fastställd bevarandetid. " bör vara i egen paragraf. Detta då den inledande texten för 26§ handlar om krav på innehåll och andra stycket om utformning samt att 27§ handlar om analys.		
kap. 3	27		Tydligör hur ofta analys bör ske.		Analyser bör åtminstone ske efter detektering enligt paragraf 38.
kap. 3	27		Se över behov att hänvisa till kap. 3 38§ och 39§.		

kap. 3	28		Utvärdera om andra stycket bör brytas ut till egen paragraf som kap.3 25§, dvs. denna del "Verksamhetsutövaren ska identifiera och hantera behovet av att använda robust och korrekt tid som är spårbar till den svenska tillämpningen av koordinerad universell tid, UTC (SP) i utvecklings-, test- och utbildningsmiljö. "		
kap. 3	30		Se över behov att en underpunkt hänvisar till paragraf 31, 32 och 33.		
kap. 3	33		I utgångspunkt bör alla ha DNSSEC men det kan, i vissa specifika fall, finnas skäl däremot.		
kap. 3	38		Se över behovet att göra andra stycket till en egen paragraf.		En egen paragraf kan skapa tydlighet. Detta då till exempel kap.3 25§ och kap. 4 8§ är utformad på detta sätt.
kap. 3	42		Se över om att göra ska-kraven som en punktlista i paragrafen.		Punktlista gör ska-kraven mer översiktliga.
kap. 3	42		Stycket om "Verksamhetsutövaren ska identifiera och hantera behovet av säkerhetsuppdateringar, uppdateringar och uppgraderingar i ot-segment." bör göras till egen paragraf.		En egen paragraf kan skapa tydlighet. Detta då till exempel kap.3 25§ och kap. 4 8§ är utformad på detta sätt.
kap. 4	5		Det är inte tydligt vad skillnaden mellan första och andra stycket är. Ska servrar som används för att bedriva sektorsverksamhet ska placeras i eget särskildt it-utrymme eller i låst skåp? Dvs. inte tillsammans med det första stycket syftar på.		
kap. 6			Det är positivt med möjlighet till undantag, men begreppet "enskilda fall" och ”särskilda skäl” är inte närmare beskrivet.	Lägg till allmänna råd med vägledande exempel på situationer där undantag kan vara aktuella, samt beskriv hur prövningen går till.