

Myndigheten för civilt försvar (MCF)
registrator@mcf.se

Stockholm 2026-05-13

Remissyttrande;

Visitans synpunkter på Förslag till Myndigheten för civilt försvars föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning (ert diarienummer MCF 2026-04554)

Visita är bransch- och arbetsgivarorganisation för den svenska besöksnäringen, med över 6 000 medlemsföretag och 8 600 arbetsställen (hotell, restauranger, contract catering, caféer, nöjesparker m.m.). Visita tecknar branschens kollektivavtal och är en medlemsorganisation i Svenskt Näringsliv. Som företrädare för de företag i besöksnäringen som bedriver samhällsviktig verksamhet har Visita ett starkt intresse av väl avvägda regelverk som förenar proportionella åtgärder för ökad cybersäkerhet med praktisk genomförbarhet.

1. INLEDNING

Visita har tagit del av Myndigheten för civilt försvars reviderade remissförslag till föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning. Vi noterar att flera förbättringar har gjorts i förslaget jämfört med det tidigare förslag som remitterades under hösten 2025 (MSB dnr 2025–13269). Myndigheten har i det nya förslaget till stor del antagit ett mer principbaserat regelverk, där exempelvis oproportionerliga detaljkrav har flyttats till allmänna råd. Visita anser att förslaget i stort är ett steg i rätt riktning som ökar flexibilitet och möjliggör en bättre anpassning till olika branschers förutsättningar.

Visita noterar dock att det finns ett antal kvarstående krav i föreskriftsförslaget som riskerar att bli oproportionerligt betungande eller otydliga i praktiken. Visita fokuserar i detta yttrande på de viktigaste områden där vi anser att ytterligare korrigeringar bör göras för att säkerställa föreskrifternas proportionalitet och praktiska tillämpbarhet.

Sammanfattningsvis anser Visita att:

- Verksamhetsutövares ansvar för interna utbildningsinsatser bör inte omfatta inhyrd personal, som snarare bör omfattas av leverantörskrav i avtal. (3 kap. 9 §)

- Bindande krav på anslutning till en specifik statlig tjänst (ANTS) bör ersättas med ett teknikneutralt funktionskrav, och kravet på leverantörsbevakning bör avgränsas till kritiska leverantörer för att möjliggöra riskbaserad prioritering. (3 kap. 10 §)
- Kravet att verksamhetsutövaren ska garantera leverantörers förmåga att uppfylla cybersäkerhetskrav under hela avtalstiden är praktiskt omöjligt och bör omformuleras. Fokus bör i stället ligga på löpande uppföljning och avtalsrättsliga sanktioner vid brister. (4 kap. 1 §)
- I de fall verksamhetsutövaren saknar rådighet över teknisk infrastruktur i sina lokaler (t.ex. vid contract catering på kunders säkerhetsklassade anläggningar) måste föreskriften tydligt medge att kraven kan uppfyllas via kravställning mot fastighetsägaren. (5 kap. 4 §)

2. YTTRANDE

2.1 Övergripande synpunkter

Visita välkomnar MCF:s mer principbaserade ansats och konstaterar att många tidigare invändningar om överdriven detaljstyrning och oproportionerlighet har beaktats. Föreskriftsförslagets utformning, med färre bundna detaljkrav, ligger mer i linje med NIS2-direktivets krav på ”lämpliga och proportionella” säkerhetsåtgärder. Det minskade antalet detaljerade skall-krav ger verksamhetsutövare större frihet att nå effektmålen på olika sätt. Ett exempel är att tvingande listor på avtalsvillkor och segmenteringskrav nu flyttats till allmänna råd i stället för bindande krav. Detta möjliggör nödvändig flexibilitet och anpassning efter riskprofil.

Samtidigt kvarstår vissa utmaningar där föreskriftsförslaget fortfarande riskerar att skapa onödig administrationsbörda eller målkonflikter. Dessa gäller särskilt inhyrd personal i interna utbildningsprogram, krav på anslutning till specifika omvärldsbevakningstjänster, leverantörskedjekrav över oförutsägbara tidsperioder samt situationen för verksamheter som inte har rådighet över driftlokaler.

2.2 Utbildningskrav för inhyrd personal

Visita delar bedömningen att all personal med systemåtkomst behöver relevant kunskap om cybersäkerhet. Visita noterar dock att 3 kap. 9 § p. 3 i sin nuvarande form likställer kraven på utbildning och övning för egen personal med inhyrd personal, även under pågående uppdrag.

Detta skapar en obefogad dubbeladministration. Inhyrda konsulter underkastas normalt de utbildningskrav som deras egna arbetsgivare (leverantören) ställer. Nödvändig kompetensstyrning avseende generell cybersäkerhet sker med fördel via leverantörsavtal och kravspecifikationer. Verksamhetsutövarens ansvar för inhyrd personal bör avgränsas till att specificera nödvändiga informationsinsatser kring lokala och specifika interna rutiner i samband med att uppdraget påbörjas. Föreskriften bör omformuleras för att undvika en onödig administrativ börda.

Visita föreslår:

- Att 3 kap. 9 § punkt 3 omformuleras enligt följande: "*3. vilka utbildningar och övningar avseende cybersäkerhet som egen personal ska genomföra, samt vilka informationsinsatser och avtalsmässiga krav som ska gälla för inhyrd personal innan och under anställning eller uppdrag.*"

2.3 Omvärldsbevakning och ANTS

Visita noterar positivt att detaljkraven avseende omvärldsbevakning har mildrats och nu möjliggör en mer riskbaserad och teknikneutral hantering, men vill samtidigt understryka två kvarstående brister i 3 kap. 10 §.

För det första innehåller paragrafen fortfarande ett tvingande och tekniks specifikt krav på anslutning till den Nationella CSIRT-enhetens notifieringar (ANTS). Detta skapar ett överlappande administrativt krav, i synnerhet då många aktörer redan har en etablerad och mer avancerad sårbarhetsbevakning via egna säkerhetsleverantörer. Kravet på just ANTS bör därför omformuleras för att medge att motsvarande informationsinhämtning sker genom andra etablerade tjänster.

För det andra ställer punkt 1 ett alltför brett krav på att bevaka "leverantörer av hård- och mjukvara" utan ytterligare avgränsning. En bokstavig tolkning innebär ett oproportionerligt och operativt ogörligt krav på att bevaka all tänkbar utrustning. Visita föreslår därför att föreskriften förtydligas så att bevakningen sker riskbaserat, och att kravet i punkt 1 uttryckligen begränsas till de leverantörer och system som identifierats utgöra en relevant risk i verksamhetens egen risk- och sårbarhetsanalys.

Visita föreslår:

- Att kravet på obligatorisk anslutning till ANTS enligt 3 kap. 10 § omformuleras enligt följande: "*Verksamhetsutövaren ska ansluta sig till automatiska notifieringar av tekniska sårbarheter (ANTS) hos den nationella CSIRT-enheten, eller säkerställa motsvarande förmåga till informationsinhämtning genom andra etablerade tjänster för sårbarhetsbevakning*".
- Att 3 kap. 10 § punkt 1 begränsas genom tillägget: "*leverantörer av hård- och mjukvara som bedömts utgöra en relevant risk i verksamhetsutövarens egen risk- och sårbarhetsanalys*".

2.4 Fysiska säkerhetsåtgärder

Visita välkomnar de förändringar som införts i 5 kap. avseende fysiska säkerhetsåtgärder, exempelvis gällande tillträde i publika miljöer. Däremot återstår en kritisk fråga i 5 kap. 3 och 4 §§ som riskerar att slå oproportionerligt hårt mot företag som arbetar utifrån en distribuerad servicemodell, på grund av bristande rådighet över lokalerna.

Enligt 5 kap. 3 § ska verksamhetsutövaren skydda lokaler mot bland annat brand och vattenskador, och enligt 4 § ska tillräcklig funktionalitet säkerställas avseende elförsörjning, kyla och ventilation. Dessa krav är problematiska för verksamheter i upplåtna lokaler. Exempelvis bedrivs många cateringtjänster (personalrestauranger, sjukhusmatsalar, skolbespisningar) i fastigheter som ägs och drivs av kunden. Dessa verksamhetsutövare kan sakna rådighet att själva genomföra och styra fastighetsinstallationer såsom reservkraft, redundant kyla eller fasta släcksystem.

Utan ett förtydligande riskerar texten att misstolkas vid tillsyn, som att verksamhetsutövaren måste ha egen fysisk rådighet över installationerna. Visita anser att föreskriftens intention uppnås om det uttryckligen medges att kraven på fysisk miljö och teknisk infrastruktur kan uppfyllas genom kravställning på fastighetsägaren.

Visita föreslår:

- Att det införs ett förtydligande i föreskriftstexten för 5 kap. 4 §, alternativt i tillhörande allmänna råd, om att verksamhetsutövare som saknar egen rådighet över lokalens fastighetstekniska system kan uppfylla kraven i 3 och 4 §§ genom avtalsmässig kravställning och samverkan med fastighetsägaren.

2.5 Leverantörskedjan och avtal

Visita välkomnar att MCF:s nya förslag har gjort omfattande och nödvändiga förbättringar gällande leverantörskrav. Visita vill dock uppmärksamma en kvarstående och problematisk formulering i 4 kap. 1 §. Där anges att verksamhetsutövaren innan avtal ingås ska ha *"bedömt att leverantören kommer att kunna uppfylla ställda krav på cybersäkerhet under hela avtalstiden."* Ett krav på att göra en långsiktig prognos över en leverantörs framtida förmåga är i praktiken mycket svårt. Kravet riskerar att leda till en kontraproduktiv osäkerhet, särskilt för mindre aktörer som upphandlar globala molntjänster, där den stelbenta formuleringen kan få verksamheter att tveka inför att använda ledande och säkra standardtjänster.

Visita anser att fokus i en bindande föreskrift bör ligga på att rätt mekanismer byggs in i avtalen, såsom krav på löpande uppföljning och tydliga sanktionsmöjligheter vid brister.

Visita föreslår:

- Att formuleringen *"under hela avtalstiden"* stryks ur 4 kap. 1 §.
- Att paragrafen omformuleras enligt följande: *"innan avtal ingås ska verksamhetsutövaren ha genomfört en riskanalys samt säkerställt att avtalet möjliggör uppföljning och specificerar åtgärder om leverantören brister i cybersäkerhet"*.

Avslutande kommentar

Visita anser att regelverket nu är betydligt mer balanserat och praktiskt hanterbart än tidigare version. Med de justeringar som föreslås ovan kan ytterligare kvarvarande målkonflikter avhjälpas, vilket skulle säkerställa att föreskrifterna blir effektiva och proportionerliga utan att överimplementera NIS2-direktivet. Visita ser fram emot fortsatt dialog i detta ärende, och ställer sig till Myndighetens förfogande för vidare samråd eller medverkan i framtagandet av riktlinjer för praktisk tillämpning av föreskrifterna.

Med vänlig hälsning



Jonas Siljhammar
VD



Mattias Svanold
Näringspolitisk Expert