

Ärendenummer
TRV 2025/127589
Motpartens ärendenummer
MSB 2025-13269

Dokumentdatum
2025-12-17

Konfidentialitetsnivå
1 Ej känslig

Mottagare
Myndigheten för samhällsskydd och
beredskap
registrator@msb.se

Kopia till
Ärendeberedning GDv
Webb- och projektstöd

Svar på remiss gällande förslag till Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning

Introduktion

Med denna skrivelse med bilaga överlämnas Trafikverkets synpunkter och reflektioner på ”förslag till nya föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning enligt kommande cybersäkerhetslag”.

Vårt bidrag fördelas på sammanfattande och övergripande synpunkter i skrivelsen samt bilagt i mer detaljerat form enligt önskad svarsmall. Skrivelsen omfattar även komplettande fördjupningsavsnitt av informativ karaktär för att ge en mer komplett kontext och bakgrund till en del av synpunkterna och förslagen till förändring. Dessa delar är inte i formell mening en del av remissvaret.

Föreskrifterna måste ses som omfattande med 76 paragrafer med underpunkter/uppräknings över 26 sidor. Till detta kommer 26 sidor konsekvensutredning. Trafikverket har bland annat av tidsskäl, MSB skickade först till en ej aktuell e-post, inte mäktat med att djupanalysera varje formulering. Trafikverket fick dock en vecka extra remisstid.

Våra sammanfattande och övergripande synpunkter kan ses indikativa och uttrycker principiella synsätt på hur författningen bör utformas och verka. Detta bör vara tillämpligt och generellt även i många fall även på ej specifikt kommenterade regleringar i den ifyllda svarsmallen

Ärendenummer
TRV 2025/127589
Motpartens ärendenummer
MSB 2025-13269

Dokumentdatum
2025-12-17

Sammanfattande och övergripande synpunkter

Inledningsvis vill vi kommentera en spretig terminologi och retorik från direktivet över lag till de tre kända förskrifterna. Vi ser utmaningar i navigat-ion bland termer, begrepp och regleringar kopplade till dessa. Synpunkter i detta avseende gäller likvärdigt för föreskrift om Incidentrapportering och informationsskyldighet.

Vissa termer delas med annan reglering exempelvis ”**viktig samhällsfunkt-ion**” utgör grunden för att identifiera **samhällsviktig verksamhet** i regelverket för civil beredskap. Inom denna disciplin förekommer företeelsen **beredskapssektorer**, enbart delvis matchande sektorer inom NIS2-direktivet.

Kärnan i NIS2-direktivet och Cybersäkerhetslagen adresserar verksamhetsutövare som bedriver **verksamhet i** någon av de **högkritiska eller kritiska utpekade sektorerna**, totalt 18 stycken. En entitet/ **verksamhetsutövare** kan vara **viktig** eller **väsentlig**. Vid anmälan ska verksamhetsutövare redovisa **anmälningspliktiga verksamheter** samt inom **vilka sektorer** och **viktiga samhällsfunktioner** verksamhetsutövaren bedriver **verksamhet**.

När verksamhetsutövarna ska jobba sig vidare med riskhantering, säkerhetsåtgärder och utbildning blir ingångsvärden i mån tu- eller tredelad. Det finns en ”tråd” från **verksamhet, sektorsverksamhet** och **sektorskritiska system** (med specifika åtgärder) som modereras något av en ansats av att etablera **lämpliga och proportionella säkerhetsåtgärder** utifrån ett **allriskperspektiv**. Kompletterande till detta så ska verksamhetsutövare **värdera sin information** (avseende K, T, R inklusive autenticitet) i **olika nivåer** utifrån vilka **konsekvenser ett bristande skydd** kan få. Till detta kopplas specificerade **åtgärder för utökat skydd** för information som bedömts ha behov av utökat skydd.

Om verksamhetsutövaren trots allt kommer fram till incidenter och skyldigheter att rapportera och informera går begreppen och retoriken över till en betydande mix. Inledningsvis tar rapporteringsplikten, i de icke sektorsspecifika delarna, sikte på **betydande incidenter** med **allvarliga störningar** i erbjudna **tjänster, ekonomisk skada** på egna och andras **verksamhet** samt betydande skador (ett flertal typer) för fysiska och juridiska personer. Vi

Ärendenummer
TRV 2025/127589
Motpartens ärendenummer
MSB 2025-13269

Dokumentdatum
2025-12-17

har **inte** noterat något om särskilda aktiviteter kopplade till sektorskritiska system. Rapportering är uppdelat i 3 faser varvid det vid upplysning fokuserar på **konsekvenser**, vid anmälan blir det centralt med **påverkan på informationens konfidentialitet, riktighet inklusive autenticitet, och tillgänglighet** samt att vid en lägesrapport vid långvarig incident beskriva om det fortfarande är **påverkan** eller det riskerar att påverka, verksamhetsutövarens egen **verksamhet**, annan **sektorsverksamhet** eller **viktiga samhällsfunktioner**.

Till alla dessa begrepp tillkommer senare ”**kritiska verksamhetsutövare**” enligt CER och eventuellt ytterligare begreppsflora.

Förslaget till föreskrifter omfattar en stor mängd krav som behöver omhändertas i det som i många fall uttrycks som interna ”regler”. Föreskrifterna är i många fall väl detaljerade. Det vore mer ändamålsenligt om kraven i föreskrifterna beskrivs på en mer övergripande nivå.

Genom att välja en så hög detaljeringsnivå finns risk att det krockar med andra regleringar. Detta är bland annat ett faktum för vår resultatenhet Färjerederiet som ser krockar med andra regleringar för fartygsoperativa OT-system och säkerhetsuppdateringar, se vidare i Excel/svarsmall.

Regleringen borde istället beskriva vad, vilken förmåga, mekanism, prestation som förväntas finnas eller uppnås. Vid ett sådant angreppssätt bör det kompletteras med ett generiskt krav om att hur man har löst uppgiften/ organiserat förmågan ska vara spårbart dokumenterat och kvalitetssäkrat i ett ledningssystem eller motsvarande. Krishantering kap2 21§ ett bra exempel.

Detta skulle möjliggöra att respektive verksamhetsutövare, inom givna ramar, kan konkretisera och anpassa kraven med hänsyn till organisationens förutsättningar. De förslagna detaljerade regleringarna gör att det är svårt att se alternativen när det gäller att arbetet med cybersäkerhet ska vara ”integrerat med befintliga sätt att leda och styra organisationen”, 2 kap 1 §.

Det finns även utmaningar i tillämpligheten om kraven i föreskrifterna skrivs på en för detaljerad nivå. Med nuvarande höga detaljeringsnivå finns risk att det krockar med andra regleringar. Vår resultatenhet Färjerederiet ser krockar med andra regleringar för fartygsoperativa OT-system och säkerhetsuppdateringar

Ärendenummer
TRV 2025/127589
Motpartens ärendenummer
MSB 2025-13269

Dokumentdatum
2025-12-17

Flera av de aktuella bestämmelsernas innehåll är mer lämpligt att utforma som allmänna råd, då de beskriver metoder och arbetssätt. Ett förtydligande i form av allmänna råd skulle ge verksamheterna större flexibilitet att välja ändamålsenliga lösningar – vilket är ändamålsenligt mot bakgrund av de olika förutsättningar som finns inom berörda organisationer. Genom att peka på ISO 27001/27002 i allmänna råd har man täckt in mycket av det som detaljeras i paragraferna – i någon mån en dubbelreglering.

Regelverket är omfattande och dess implementering kan få stora konsekvenser för berörda myndigheter och organisationer. Regelverket påverkar såväl ledning och styrning, interna regelverk, kompetensbehov som krav på systemstöd. Vi tycker oss se utökade krav administrativa åtaganden kring dokumentation och monitorering och teoretisk övervakning av risker och åtgärder. I många fall är detta kopplat till frekvens eller givna intervall på aktiviteter. Även om detta ur en principiell utgångspunkt är rimligt och en grund i att bygga cybersäkerhetsförmåga bör man se upp så att vi inte får en tyngdpunkt på administration på bekostnad av reell och teknisk förmåga att stå emot cyberhot.

Att kravställa ledningens ansvar när det gäller kunskap, förståelse och engagemang i riskbaserade och systematiska arbetssätt inom området på någon nivå är helt rimligt. Olika stora organisationer kan inte ha samma detaljer/djup i ”ledningens” direkta verkan. Rimlighet att göra ledning ansvarig för operativa aktiviteter likt ”Ledningen ska tydliggöra vem som ansvarar vilken informationsbehandling” i stora organisationen med omfattande informations- och IT-landskap. Det kan handla om hundratals objekt som dynamiskt ska kopplas till ansvariga i ett IT-och informationslandskap som är i ständig transformation. Återigen utmaning med verksamhetsutövare olika storlek och uppdrag.

Vem är ledningen? Vi har inte hittat att det inte framgår explicit i föreskriften men andra källor ger indikationer att följande avses: för aktiebolag, styrelse och vd; för statliga myndigheter, generaldirektören och de anställda som utövar ledningsfunktioner; för regioner och kommuner, regions- eller kommunstyrelse. Vi noterar i sammanhanget att Myndighetsförordningen (2007:515) beskriver att styrelsen är ledningen i styrelsemyndigheter. Låt verksamhetsutövare tolka och dokumentera ledning och ledningsfunktioner samt dokumentera hur ansvar och arbetsuppgifter fördelas – ingen hård reglering

Ärendenummer
TRV 2025/127589
Motpartens ärendenummer
MSB 2025-13269

Dokumentdatum
2025-12-17

Vi har gjort en reflektion över att man konsekvensbeskrivningen i propositionen föreslår att kostnaderna för de offentliga verksamhetsutövarna ska finansieras inom befintlig ram. Utredningen anser att det är rimligt att offentliga verksamhetsutövare vidtar grundläggande säkerhetsåtgärder. Detta ställer sig i viss mån verbalt i kontrast till direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå. Sett i detta perspektiv är det inte uppenbart hur föreskrifterna bidrar till en balansering mellan grundläggande säkerhetsåtgärder och en hög gemensam cybersäkerhetsnivå. Här skulle förstås mekanismen om att ”genomföra lämpliga och proportionella säkerhetsåtgärder utifrån ett allriskperspektiv” kunna kliva in men det är inte uppenbart hur den ansatsen verkar med samtliga indispositiva krav på åtgärder i föreskriften.

Bland annat mot tidigare resonemang kring integrering med befintliga sätt att leda och styra organisationen” (2 kap 1§) ser Trafikverket en utmaning i att ”minst utse roller motsvarande samordnare, informationsägare och systemägare”. För att integreringen (2 kap 1§) på allvar ska fungera måste kravställningen lyftas till vilka förmågor, nyttor, effekter som ska verksamhetsutövaren ska inneha/uppnå.

Regleringen bör istället beskriva vad, vilken förmåga eller mekanism som förväntas finnas. Behöver inte realiserats med specifikt som ”roller” utan skulle kunna vara beskrivet som ett arbetssätt eller systematik. Exempelvis för ”samordnare” borde detta kunna uttryckas som: verksamhetsutövaren ska ha förmåga genom etablerad systematik (etablerade strukturer/mekanismer/arbetssätt) samordna och utvärdera arbetet med och nytta/effekt av (säkerhets-)åtgärder som stöd till ledningens ansvar för att leda och styra cybersäkerhet.

Det förekommer exempel på regleringar som i stor utsträckning följer ovan beskriven logik med att formulera sig i förmågor. Exempelvis 2 kapitlet 21§ om krishantering som inledningsvis beskriver vilken förmåga och effekt som eftersträvas och sedan vilka nedbrutna förmågor/egenskaper som ska ingå samt att det ska vara dokumenterat. Dock finns fler sätt att formalisera dokumentation än enbart genom ”regler” (rutiner, arbetssätt, mekanismer, mm)

När det gäller information är det centralt att verksamhetsutövaren har förmåga att klassa och riskhantera information för ett för verksamhetsutövare ändamålsenligt och relevant sätt. Att detta ska samlas till en roll ”motsvarande” informationsägare kan inte vara avgörande. Med god härledning har

Ärendenummer
TRV 2025/127589
Motpartens ärendenummer
MSB 2025-13269

Dokumentdatum
2025-12-17

Trafikverkets hittills beslutat att interna informationsägare inte ingår ledningssystemet. Se vidare om avsnitt "Fördjupat om informationsägare" och dito för systemägare i det informativa avsnittet sist.

Bilagor

1 - Informativa och fördjupande kompletteringar

Direkt efterföljande i detta dokument

2 - Svar i Excel-mall

Bifogat i "msb-2025-13269-svar-Trv-föreskrifter-säkerhetsåtgärder-o-utbildning" återfinns efterfrågade detaljerade noteringar på "paragrafnivå". Samtliga förändringar som behöver följa på de mer principiella förändringsbehoven som framgår i skrivelsen som innevarande brev utgör är bara delvis inarbetade i bilagd Excel.

Beskrivning av handläggningen

Beslut har fattats av Chef central funktion Säkerhet Mattias Dejke.

Föredragande har varit Lars Lundmark, Senior säkerhetsstrateg och riskrådgivare, central funktion Säkerhet.

Organisationen har inbjudits att bidra via ärendebrevlådor på verksamhetsområden, centrala funktioner och resultatenheter. Inkomna synpunkter har vägts samman och sammanställts av föredragande enligt ovan. Löpande dialog har skett med Alice Dahlquist, strateg Verksgemensam styrning.

Mattias Dejke

Chef central funktion Säkerhet

Lars Lundmark

Senior säkerhetsstrateg och riskrådgivare

lars.lundmark@trafikverket.se

Direkt: 010-123 10 06

Ärendenummer
TRV 2025/127589
Motpartens ärendenummer
MSB 2025-13269

Dokumentdatum
2025-12-17

Trafikverket

Adress: 781 89 Borlänge

Besöksadress: Röda vägen 1

Ärendenummer
TRV 2025/127589
Motpartens ärendenummer
MSB 2025-13269

Dokumentdatum
2025-12-17

Bilaga 1

Informativa och fördjupande kompletteringar

Särskilt om "informationsägare"

Så vitt vi känner till finns det ingen legaldefinition av "informationsägare". Det närmaste man kommer principiellt finns nog inom immaterialrätten samt med lite principiell tolkning inom dataskydd och integritet. Det närmaste man koppla "informationsägande" till skulle i så fall vara fysiska eller juridiska personer.

I en alltmer digitaliserad värld (objektifierad, inte primärt sammansatta objekt som handlingar/dokument), digitalisering, TOP The once and only principle, Analys/BI, Initiativ kring Dataspaces och öppna data. Information/data kan byggas ihop med annan information till ny information i oändliga iterationer. Samma typ av information kan därför förekomma i många sammansatta objekt

Interoperabilitet ökar behovet att adressera gemensamhet i frågor om betydelse, struktur, kvalitet, etc ökar desto fler aktörer och sammanhang som hanterar informationen Samtidigt som frågor inom riskhantering och säkerhet samt informationsredovisning (handling) och bevarande/ gallring fortsätter att kräva tydlig koppling till aktör och sammanhang/kontext distribuerat i organisationen och/eller processer.

Samma typ av information (informationsobjekt) kan förekomma i många olika verksamheter, inom egen organisation, där man kan behöva **en ansvarig** ("ägare") för struktur/betydelse ur governance för masterdata och samtlig hantering men där klassning framförallt tillg. och rikt. högst troligt skiljer sig beroende på vilket verksamhetskontext informationstypen/-objektet hanteras/förekommer. Ett, helst dokumenterat kontext För att kunna svara på frågan "vad blir verksamhetskonskvensen om...". Det betyder att information behöver/kan behöva flera andra **ansvar** ("ägare") som klassar information (samma typ) beroende på var den förekommer i organisationen eller processer.

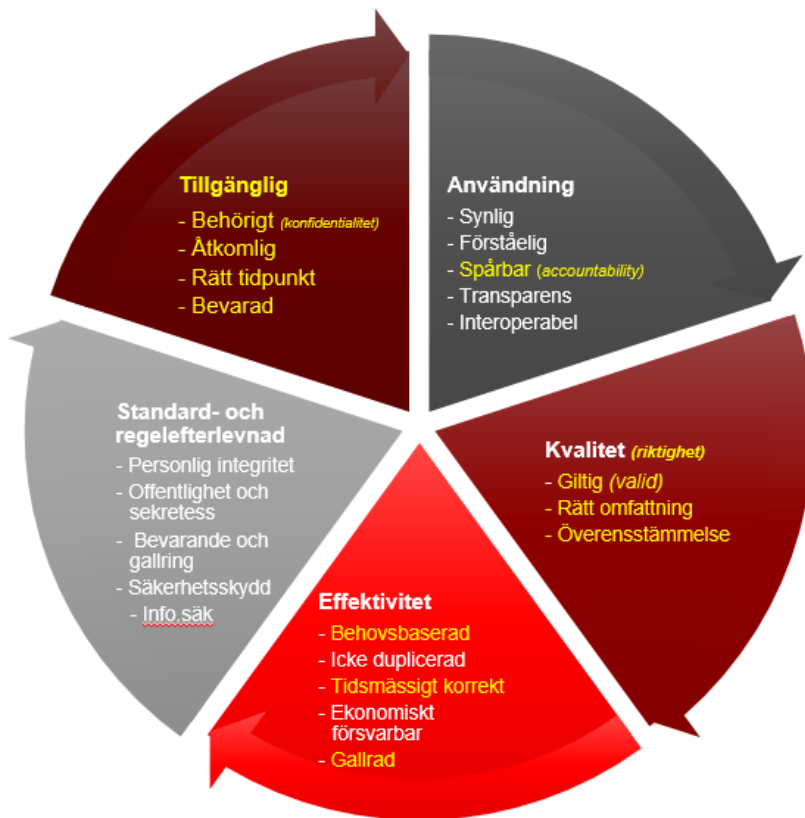
Det är dessutom så beroende på användning är det troligt att informationstyper (ur ett innehållsperspektiv) sätts samman i olika nya objekt/samlingar

Ärendenummer
TRV 2025/127589
Motpartens ärendenummer
MSB 2025-13269

Dokumentdatum
2025-12-17

(aggregat och ackumuleringar) för vilka det kan finnas en specifik verksamhetskontext och skäl till en ny klassningspunkt och ett nytt **ansvar** ("ägare") som klassar information.

En organisation kan jobba mot en vision om "Rätt information till rätt aktör vid rätt tillfälle" (även på "rätt sätt") där systematik för att hitta "rätten" ska bland annat betraktas och utformas med utgångspunkt ur synvinklarna/ aspekterna: Konfidentialitet Tillgänglighet och Riktighet men integrerat med övriga dimensioner inom effektivitet, kvalitet, informationsredovisning, bevarande/gallring, interoperabilitet, digitalisering, etc.



TMALL 0422 Brev 4.0

Det är möjligt att de ansvar och uppgifter ni ger "informationsägare" ingår i andra roller och befattningar med ett bredare perspektiv – exempelvis tjänsteansvarig/-ägare, processansvarig/-ägare, produktägare, och informationsförvaltare. Det är också möjligt att efterfrågade förmågor kan byggas av andra delar i ett ledningssystem utan att använda sig av "roll"

Ärendenummer
TRV 2025/127589
Motpartens ärendenummer
MSB 2025-13269

Dokumentdatum
2025-12-17

Det är en utmaning att för stort fokus läggs på den **där enda informations-ägaren**. Det skapar oönskade låsningar (se även kommentar 7§ 2 kap9). Det väsentliga är att systematik och principer i en organisation är beskriven (i linje med hur verksamheten i övrigt styr och leder §1.)

Det kan också förekomma systematik där man, i första hand för strukturerad objektifierad info/data, skiljer på ansvar för typobjekt till vilka man definierar egenskaper och krav samt hanterandeansvar för instanser/förekomster av typen. Någon har ansvar för att beskriva hur "Kund" ska beskrivas och kravställas men de faktiska kunduppgifterna hanteras producenter och konsumenter runt om i organisationen/processerna. De är förekomsterna som utsatt för risk därav följer ansvar för riskbehandlings-/säkerhetsåtgärder till de som hanterar förekomster ofta även inkluderande ansvar för, eller kravställande på, de inblandade informationsbehandlingsresurserna. Dessa ansvar behöver inte vara samma ansvarig som för typobjektet.

Utmaningar med systemägare och "system" som objekt för krav och tvingande moment

Återigen vad avses med "system". I någon skulle kraven på dokumentation per "system" vara rimlig i ett IT-landskap bestående av stordatorsystem a 'la 70-tal. Idag i ett modernt IT-landskap är "system" inte lika självdefinierande. Idag är det mycket mer modulärt uppbyggt och komponenter kan ingå i komponenter eller system i system.

System kan utgöra plattform för flera andra system, en skiktad arkitektur. En skiktad arkitektur med applikationer med verksamhetslogik som tillsammans med flera andra applikationer "hostas" på applikationsplattformar som i sin tur kanske nyttjar och delar lagringskluster/-plattformar med fler. Varje lager kan ha olika verksamhetsansvar och riskägarskap.

Exempelvis. Vi har en Sharepoint-plattform som i sig kan ses som ett system men på den har det satts upp ca 56 applikationer (konfigureringar) som var för sig ur ett förvaltningsperspektiv förvaltas (i viss mån jmf med "ägare" i vissa avseenden) av olika ansvar i organisationen. Det är dessutom så att alla 13-14 måsten under kap 3 8 § är inte relevant att dokumentera "för varje system", det är beroende på var "systemet" befinner sig i arkitekturen.

Ärendenummer
TRV 2025/127589
Motpartens ärendenummer
MSB 2025-13269

Dokumentdatum
2025-12-17

Dokumentegenskaper, Ärendenummer TRV 2025/127589, Motpartens ärendenummer MSB 2025-13269, Dokumentdatum 2025-12-17, Dokumenttyp BREV. Konfidentialitetsnivå.1 Ej känslig

Ovanstående textfält är endast avsett att läsas digitalt och får ej tas bort. Det innehåller uppgifter från sidhuvudet och gör att dokumentets egenskaper blir tillgängliga enligt Lag (2018:1937) om tillgänglighet till digital offentlig service.