Sveriges universitets-
och högskoleförbund
Tryckerigatan 8
111 28 Stockholm

2025-12-05
Dnr. SU-850-0054-25
Synpunkter

Myndigheten för samhällsskydd och beredskap

Synpunkter på förslag till Myndighetens för samhällsskydd och beredskaps föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning samt föreskrifter om incidentrapportering och informationsskyldighet

Sveriges universitets- och högskoleförbund (SUHF) yttrar sig härmed över Förslag till myndighetens för samhällsskydd och beredskaps föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning (MSB 2025-13269), bilaga 1, samt Förslag till myndighetens för samhällsskydd och beredskaps föreskrifter om incidentrapportering och informationsskyldighet (MSB 2025-13324), bilaga 2. Yttrandet lämnas mot bakgrund av bedömningen att flera av Sveriges lärosäten kommer att omfattas av kommande Cybersäkerhetslag.

Inledning

Sveriges lärosäten arbetar med att stärka sin cybersäkerhet. Det är ett prioriterat arbete som bedrivs med kraft och genom såväl administrativa åtgärder som genom att sätta av personella och ekonomiska resurser. SUHF välkomnar således regeringens förslag till Cybersäkerhetslag då denna tydligt stödjer detta arbete. De synpunkter som lämnas är framtagna utifrån en bedömning av att, som framför allt förslaget om säkerhetsåtgärder och utbildning är skrivet, kommer berörda verksamhetsutövare att oundvikligen omfördela resurser från verkligt riskreducerande arbete som en enkel tydlig styrning, tekniska skydd och kontinuerlig förbättring till att leva upp till formaliteter. Detta kommer dels att hämma det löpande arbetet, dels kraftigt försena implementeringen av reella cybersäkerhetsåtgärder.

Regering och riksdag är tydliga med att det är nödvändigt med åtgärder för att främja Sveriges konkurrenskraft och därmed bevara och utveckla Sveriges välfärd. I linje med detta har riksdagen trots det ansträngda finansiella läget beslutat om ytterligare stora satsningar på forskning och utveckling; ett anslag som redan är cirka femtio miljarder kronor per år. Satsningarna sker bland annat på biobanker, forskningsdatabaser och artificiell intelligens, men också satsningar som MAX IV, ESS och SciLifeLab. Regeringen är också i till exempel Digitaliseringsstrategin 2025-2030, tydlig med dess intentioner att driva en offensiv förenklingsagenda. Det är helt linje med AI-kommissionens bekymrade konstaterande (SOU 2025:12) om de befintliga detaljerade och krångliga regelverk som hindrar möjligheterna att få full avkastning på de satsningar som görs. I detta läge är det mycket bekymmersamt att MSB lämnar förslag om ytterligare sådana regleringar.

Övergripande synpunkter

Av såväl NIS 2-direktivet som förslaget till Cybersäkerhetslag framkommer att verksamhetsutövare ska vidta lämpliga och proportionella säkerhetsåtgärder och att de ska utgå från ett allriskperspektiv samt säkerställa en nivå på säkerheten som är lämplig i förhållande till risken. SUHF menar att på grund av en alltför hög detaljeringsgrad så strider framför allt

förslaget till säkerhetsåtgärder och utbildning mot dessa grundläggande principer. En hög detaljeringsgrad är helt olämplig i en reglering som gäller för såväl stora och små statliga myndigheter som kommuner och privata företag och resulterar såväl i för hög som för låg nivå av säkerhet. Om förslagen realiseras menar vi att det försvårar möjligheten för svenska forskare att bedriva den excellenta forskning som är nödvändig för vår välfärd.

Föreskrifterna bör generellt reglera vad som ska uppnås och inte detaljstyra hur detta ska göras. SUHF vill som ett exempel på mer generell problematik lyfta det för lärosätena särskilt besvärande med ”informationsägare” och ”nformationsklassning”. På ett lärosäte kan det finnas tiotusentals forskningsprojekt och det är givetvis den enskilde forskaren som bäst känner till vilken information som ingår i varje forskningsprojekt. I den meningen bör det vara den enskilde forskaren som är ”informationsägare”. Det faller på sin egen orimlighet att då stipulera att *Interna regler ska minst ange 1. att riskanalys genomförs a) innan information behandlas i system, och b) vid förändrade hot och nya sårbarheter, 2. att uppgiften att initiera arbetet med och fastställa resultatet av riskanalysen utförs av a) informationsägaren avseende den information som denne ansvarar för, och b) systemägaren avseende de system och de delar av den digitala miljön som denne ansvarar för*. Resultatet skulle bli att på ett stort lärosäte ska var och en av de tusentals forskare som finns genomföra en riskanalys. Det är också orimligt att en forskare som informationsägare *ska bedöma behovet av att behandla information under störda förhållanden utifrån vad som är acceptabla tider för nedsatt funktionalitet och otillgänglighet för verksamheten.* Detsamma gäller *Innan ett beslut om att för första gången driftsätta ett system ska fattas, ska systemägaren minst kontrollera att … informationsägaren har beslutat om att påbörja behandlingen av information*.

I första hand kan problematiken lösas genom att föreskrifterna överhuvudtaget inte anger specifika roller som i det här fallet ”informationsägare”. I stället bör det generella anslaget vara att ”verksamhetsutövaren ska tillse”, ”verksamhetsutövaren ska initiera” och så får respektive verksamhet bedöma hur det hela ska uppnås. En andrahandslösning – som sannolikt är sämre – vore att tydliggöra att verksamheten kan utse informationsägare som genomför en ”informationsklassning” av typer av information och att sådana typer av information ska behandlas med vissa skyddsåtgärder. Det skulle i sammanhanget vara angeläget att en verksamhet kan fatta besluta om typer av information som inte behöver klassas överhuvudtaget. Det finns mycket forskning där det inte är meningsfullt att lägga resurser på informationsklassning, t ex om latinets utveckling under 1200-talet. Det skulle i så fall av föreskriften behöva framkomma att lärosätet ska säkerställa att all forskningsdata har ett visst grundskydd så att den inte riskerar förstöras, men det kan uppnås utan informationsklassning.

SUHF vill även för lärosätenas del lyfta att de föreslagna föreskrifternas krav på säkerhetsåtgärder i flera avseenden inte är avgränsade till den verksamhet och de system där de är lämpliga. Vissa av kraven kan utgöra betydande hinder för att exempelvis utveckla programvara eller IT-system inom ramen för forskning och utbildning.

Fler synpunkter lämnas i de två bilagorna. Yttrandet har beretts av Arbetsgruppen kring införandet av cybersäkerhetsreglering.

Enligt uppdrag

Marita Hilliges
generalsekreterare