KONSTFACK
University of Arts, Crafts and Design

Remissvar **IT-avdelningen**
2020-02-20 Handläggare: A Amling
Dnr KF2019/VO1/44 IT-chef

Svar på remiss ”Förslag till nya föreskrifter om informationssäkerhet och IT-säkerhet för statliga myndigheter ” från MSB

Bakgrund

MSB skickade den 18:e december 2019 ut förslag till nya föreskrifter om informationssäkerhet och IT-säkerhet för statliga myndigheter.
Dessa förslag kan på en övergripande nivå sammanfattas med:

- Alla statliga myndigheter omfattas dvs även U/H-sektorn i stort.
- Förslagen till föreskrifter gör ingen skillnad på vilken verksamhet som en myndighet bedriver utan definierar en ”bottenplatta” för samtliga.
- Förslaget är att de förändrade föreskrifterna börjar gälla från den 1:a juli 2020, om mindre än 6 månader. Föreskriften börjar gälla direkt och myndigheten riskerar därför att bryta mot föreskrifterna direkt vid ikraftträdandet. Detta innebär en tidsfrist som upplevs som oskälig för de flesta lärosäten, eftersom det blir en stor utmaning att hinna genomföra de anpassningar som krävs enligt förslaget.
- Centrala begrepp är att arbetet ska bedrivas på ett systematiskt och riskbaserat sätt. Detta innebär även att alla medarbetare ska informationsklassa information, att myndigheten arbetar med riskanalyser, inför lämpliga säkerhetsåtgärder och följer upp samt utvecklar informationssäkerhetsarbetet. Detta jämförs med arbetet med ISK men även med arbete med kvalitetssystem.

Den 14:e januari 2020 genomförde IT-chefsnätverket ett möte där ett 25-tal deltagare från olika lärosäten deltog. Förslagen diskuterades kort och man enades om att utse en arbetsgrupp, bestående av Linköpings universitet, Lunds universitet, Uppsala universitet, Mälardalens högskola och Kungliga musikhögskolan. Efter detta har även Stockholms universitet anslutit. Målet för arbetsgruppen har varit att gemensamt arbeta fram ett förslag på text som lärosätena är fria att inkorporera i sina respektive egna remissvar. Huvudtanken med den gemensamma skrivningen är att tydliggöra den särart som U/H-sektorn har. U/H-sektorn har en gemensam utmaning i både verksamhetens karaktär, varierande storlek och därmed vilka resurser som finns till förfogande men även i myndighetskultur (t.ex. styrning och ledning av verksamheten).

Gemensamma huvudsynpunkter från deltagande lärosäten

Huvudpunkter att beakta:

- U/H-sektorns förutsättningar rörande forskning och undervisning.
- Föreskrifterna, främst den om IT-säkerhet, behöver vara hållbara över tid. Att med regelbundenhet (på något/några år) behöva uppdatera föreskriften skapar inte långsiktighet.
- Detaljnivån i föreskrifterna för IT-säkerhet är både för detaljerad och för oexakt. Sannolikt vore det bättre att beskriva vad syftet med en viss regleringen och vilken effekt som avses uppnås istället för att beskriva exakt hur.

Myndigheten har mottagit förslagen på nya föreskrifter rörande informationssäkerhet och IT-säkerhet. Inledningsvis konstateras att området är angeläget och att alla förtydliganden av vikten för området välkomnas. Samtidigt konstateras att föreliggande förslag gäller samtliga statliga myndigheter utan hänsyn till respektive myndighets unika förutsättningar, storlek och verksamhet.

Universitet och högskolesektorn har gemensamma utmaningar i synen kring forskning och undervisning i förslagen till föreskrifter. Dessa utmaningar tar sin utgångspunkt från att högskolan i enlighet med Högskolelagen (1992:1434) 1 kapitlet §2 har tre uppgifter; utbildning, forskning och samverkan med det omgivande samhället. Dessa är alltså högskolans primära och huvudsakliga uppgifter.

Föreskriften för IT-säkerhet använder termen produktionssystem. Termen är inte närmare definierad utan den måste tolkas. Den initiala tolkningen är att den minst omfattar informationssystem som är centrala för myndighetens ”produktion”. Med hänsyn till högskolelagen innebär detta att de lösningar och IT-system som används och utvecklas inom ramen för forskning och undervisning är att betrakta som produktionssystem. Det vill säga en högskolas ”produktion” är forskning och undervisning. Detta synsätt bedöms utgöra en omfattande påverkan på möjligheten att bedriva forskning och undervisning. I högskolelagen 1 kap. §3 står att verksamheten ska bedrivas så att det finns ett nära samband med forskning och utbildning. Detta innebär att även övrig verksamhet, så som administration och teknisk verksamhet, påverkas av huvuduppgifterna för högskolan. En särskild utmaning är det, ofta, starkt decentraliserade ansvaret som finns inom många lärosäten. Slutsatsen blir, att trots att förskrifterna i stort innehåller många positiva förslag behöver dessa ses över på ett sådant sätt att de inte hindrar den fria forskningen och riskerar utbildningens kvalitet.

I allmänhet konstateras även att det är av vikt att föreskrifterna är hållbara över en längre tid. Anledningen till detta är att skapa förutsättningar för en långsiktig planering. I förekommande fall bör därför specifik reglering bytas ut mot vilken effekt som eftersträvas i stället för en reglering i form av en mer exakt lösning.

Härutöver föreslås föreskrifterna börja gälla omedelbart vid ikraftträdande vilket riskerar att innebära att myndigheten, i likhet med andra högskolor, kommer bryta mot föreskriften

direkt. Det är därför angeläget att det finns tid till anpassning innan föreskriften börjar gälla. Vårt förslag är att föreskrifterna för informationssäkerhet och IT-säkerhet börjar gälla som rekommendationer från 1:a juli 2020 men träder i kraft som en skarp föreskrift först 1:a januari 2022.

Myndigheten ska enligt föreskriften om informationssäkerhet arbeta systematiskt och riskbaserat med informationssäkerhet, men föreskriften rörande IT-säkerhet begränsar möjligheten att göra det eftersom man redan bestämt sig för att för vissa delar behandla all information enligt specifika tekniker.

Exempelvis finns ingen flexibilitet att uppnå mål som beskrivs i förordningen med andra medel eller lösningar, vilka kan vara minst lika effektiva men på andra sätt bättre för verksamheten.

Det finns inte heller någon möjlighet att bedöma om en viss åtgärd är proportionerlig för den enskilda myndigheten.

Det systematiska informationssäkerhetsarbetet ska enligt föreskriften om informationssäkerhet bedrivas med stöd av ISO 27000, men föreskriften om IT-säkerhet saknar koppling till ISO 27000. Resultatet är att myndighetens informationssäkerhetsarbete ska vara riskbaserat samt bedrivas med stöd av etablerade standarder. Men i många viktiga aspekter kan inte arbetet ta någon hänsyn till detta eftersom IT-säkerhetsföreskriften i detalj föreskriver åtgärder.

Konstfacks enskilda remissvar

Konstfack har mottagit ovanstående remiss. Myndigheten redovisar utöver ovanstående synpunkter sitt enskilda svar nedan på remissen samt bifogar två ifyllda svarsmallar som medföljde remissen.

Det konstateras att föreliggande förslag gäller samtliga statliga myndigheter dvs även U/H-sektorn i stort, utan hänsyn tagen till respektive myndighets unika förutsättningar, storlek, verksamhet eller vilken information man hanterar.

Vi rekommenderar att föreskrifterna utformas så att de ger utrymme för myndigheternas egna bedömningar i val av teknik för IT-säkerhet med utgångspunkt från informationssäkerhetsarbete och riskanalys.

Föreskrifterna måste även kunna uppfyllas samtidigt som de måste vara proportionerliga i förhållande till myndighetens tillgängliga resurser. Detta så att även mindre lärosäten/myndigheter har möjlighet att uppfylla föreskriften.

- Vi anser det helt orimligt att föreskrifterna ska börja gälla så snabbt dvs om *mindre än 6 månader*.

För Konstfack som är en liten högskola och med mycket begränsade resurser innebär förslaget att det inte är möjligt att med dessa både hinna och kunna uppfylla de krav som anges.

Om föreskrifterna börjar gälla 1/7 2020 kommer lärosätet direkt att bryta mot föreskrifterna.

Om förslaget till föreskrifterna verkställs i nuvarande form den 1/7 2020 behöver extra resurser tillföras myndigheten för att kunna uppfylla föreskriften.

Vi rekommenderar att föreskriften med vissa justeringar är en rekommendation from 1/7 2020 och att de börja gälla tidigast 1/7 2022. Även med detta tidsperspektiv kan det vara svårt att med befintliga resurser kunna förvalta de krav som anges i nuvarande förslag.

- **Vi vänder oss starkt emot den detaljnivå som** anges i föreskrifterna för IT-säkerhet där det i många fall definieras exakt vilken teknik eller lösning som ska användas oavsett informationsklassificering.

  Föreskrifterna för informationssäkerhet anger att myndighetens informationssäkerhetsarbete ska vara riskbaserat och bedrivas med stöd av etablerade standarder. Det innebär att man först efter en informationsklassning och riskbedömning av innehåll i IT-systemen kan göra en bedömning av vilken teknisk lösning som är mest lämplig för att uppnå det aktuella skyddsbehovet. Att i förväg fastställa vilken tekniklösning som måste användas är att gissa och blir sannolikt inte heller kostnadseffektivt eller motsvarar rätt skydd.

  *Vi rekommenderar att föreskrifterna beskriver **vad syftet är med en viss reglering och vilken effekt som avses uppnås** istället för att beskriva exakt hur.*

- Vissa **begrepp** är knapphändigt definierade i föreskriften vilket gör det svårt att bedöma hur kravet ska tolkas.

  Vi rekommenderar att om fler facktermer används i texten än de redan angivna i listan med begreppsförklaring att dessa läggs till i listan.