Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

YTTRANDE SLU ID: SLU.ua.2019.2.6-5198

2020-02-14

registrator@msb.se

Yttrande över remiss från Myndigheten för samhällsskydd och beredskap om deras föreskrifter om informationssäkerhet samt om it-säkerhet för statliga myndigheter (dnr. 2019/14545 och 14546)

Sammanfattning

Sveriges lantbruksuniversitet, SLU, har mottagit förslagen på nya föreskrifter rörande informationssäkerhet och it-säkerhet. Inledningsvis konstateras gemensamt med andra universitet och lärosäten, 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

Postadress: Box 7070, 750 07 Uppsala
Besöksadress: Almas allé 8
Org nr: 202100-2817
www.slu.se

Tel: 018-67 10 00 (vx)
Mobilnr: 070-544 1674
Fredrika.von.sydow@slu.se

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. Förslaget är att föreskrifterna för informations-säkerhet och IT-säkerhet börjar gälla som *rekommendationer* från 1:a juli 2020. Ett ikraftträdande behöver dock föregås av en djupare analys av hur forskningsområdet i stort ska hanteras.

Myndigheten ska enligt föreskriften om informationssäkerhet arbeta systematiskt och riskbaserat med informationssäkerhet, men föreskriften rörande IT-säkerhet begränsar möjligheten att göra det. Exempelvis finns ingen flexibilitet att uppnå mål som beskrivs i förordningen men 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.

SLU bedömer att det råder osäkerhet i förmågan att säkerställa efterlevnaden av de föreslagna föreskrifterna, beroende på i huvudsak följande oklarheter:

- Tidshorisont: SLU ser det som en omöjlighet att till föreslagna ikraft-trädande 1 juli 2020 säkerställa att föreskrifterna efterlevs. Detta dels på grund av tekniska anpassningar, dokumentationskrav, harmoniseringen mellan föreskrifterna och att delvis nya samverkansrutiner måste etableras inom myndigheten. Dessutom bedömer SLU att den av MSB genomförda konsekvensanalysen, inte tar höjd för de faktiska inköpskostnader som uppstår för omställningen för lärosäten.
- Definitioner: För att fokusera rätt i implementationsarbetet skulle det behöva tydliggöras och avgränsas vad som avses med t.ex. *informations-säkerhet* samt *produktionsmiljö* respektive *utvecklings- och testmiljö.* Det finns tolkningsutrymmen huruvida t.ex. applikationer till mobiltelefoner

utgör informationssystem eller om exempelvis applikationer i forskningssyfte ingår i produktionsmiljö eller testmiljö.

- Avgränsning: Det behövs en generell avgränsning av kravens tillämpning till att gälla sådana system som myndigheten bedömer som kritiska för verksamheten eller av annan befullmäktigad part bedöms som kritiska ur ett samhällsperspektiv.
- SLU ser generellt stora utmaningar i möjligheten att applicera de föreslagna föreskrifterna på de delar av vår verksamhet som rör forskning. Denna utgör tillsammans med undervisning och samverkan med det omgivande samhället, SLU:s grunduppdrag. SLU önskar därför att MSB inbjuder till en kompletterande dialog kring de förutsättningar som råder för forskning och utveckling inom svenska lärosäten.

Generella synpunkter

SLU är ett universitet som i samverkan med andra kan göra skillnad i omställningen till ett hållbart samhälle. Den digitala utvecklingen är en genomgripande global samhällsförändring som påverkar det mesta i vår vardag. För oss som universitet ger den många nya möjligheter och ett övergripande mål är därför att SLU använder den digitala utvecklingen för ökad kvalitet i utbildning, forskning och miljöanalys. En viktig komponent är hur stora datamängder kan användas för att utveckla ny kunskap som ligger till grund för tolkning och förståelse av komplexa system. Digitalisering kan också bidra till ”öppen vetenskap” där information och kommunikation av forskningsresultat och underliggande data tillgängliggörs och förädlas av våra studenter, intressenter och samhället i stort.

Universitetsvärlden styrs av förutsättningar som i flera avseenden skiljer sig från mer traditionella myndighetsaktiviteter, varför de föreslagna föreskrifterna inte ses som fullt ut tillämpliga i nuvarande utformning på universitet och högskolor. Det krävs t.ex. en större anpassbarhet för att applicera föreskrifterna på forskningsområdet. SLU ser däremot positivt på förskrifternas ambition att förtydliga och öka IT-säkerheten generellt.

Vad gäller MSB:s förslag till föreskrifter samt allmänna råd om informationssäkerhet för statliga myndigheter önskar SLU lämna följande synpunkter:

Begreppsförklaring 3§
För att fokusera rätt i implementationsarbetet skulle det behöva tydliggöras och avgränsas vad som avses med t.ex. informationssäkerhet, produktionsmiljö samt utvecklings- och testmiljö. Det bör framgå om laborations- och forskningsmiljö utgör produktionsmiljö, testmiljö eller om ytterligare någon miljö avses.

Utkontraktering §§4-6
Bestämmelsen syftar endast på när en myndighet överlåter till annan myndighet att utföra uppgifter enligt denna författning. Det finns ett behov av att reglera vad som ska gälla när en myndighet uppdrar åt annan myndighet att ta fram information i

egenskap av t.ex. expertkompetens. Det bör framgå var ansvaret för att informationsklassa informationen ska ligga, antingen hos den myndighet som ger uppdraget eller den myndighet som utför uppdraget. Informationsägarskapet behöver tydliggöras.

Fysiskt skydd och personalsäkerhet 14-16§§
SLU föreslår att myndigheten utifrån riskbedömning alternativt informationens *värde*, ska vidta säkerhetsåtgärder som försvårar obehörigt tillträde till myndighetens lokaler där information hanteras. De flesta lokaler innehar datanät, Wifi, klienter m.m. så en eventuell klassning på lokal skulle se likadan ut för alla lokaler, undantag där säkerhethetsskyddade uppgifter finns eller där server/korskopplingsrum finns.

§16 Det behöver förtydligas vilka aktiviteter som avses med bakgrundskontroller.

Uppföljning av informationssäkerhet 17-18§§
§17 punkt 3 Då kravet på ledningssystemet för informationssäkerhet är uttryckt som att det ska ta stöd i nämnda standarder ställer sig SLU frågande till det föreslagna kravet att årligen sammanställa skillnaden mellan införda säkerhetsåtgärder och säkerhetsåtgärder preciserade i standarderna S-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017. Vidtagna säkerhetsåtgärder borde lämpligen jämföras med de säkerhetsåtgärdsbehov som identifierats av myndigheten genom genomförda informationsklassningar och riskbedömningar av informationssystem som myndigheten bedömt som verksamhetskritiska.

Vad gäller MSB:s förslag till föreskrifter om it-säkerhet samt allmänna råd önskar SLU vidare att lämna följande synpunkter:

1 kap. Inledande bestämmelser

Tillämpningsområde 1-2§§
Det bör göras en åtskillnad mellan olika myndigheter då förutsättningarna är väldigt olika och verksamheterna skiljer sig stort mellan forskningsdriven verksamhet och mer traditionell myndighetsverksamhet.

2 kap. Hantering av säkerhet i informationssystem

Ansvar, kompetens och resurser 2-4§§
Om applikationer till mobiltelefoner samt forskningsverksamhet utgör informationssystem bedömer SLU att det krävs orimliga insatser för att efterleva kravet.

Bedömning av risk 5-6§§
En avgränsning av kravet önskas genom följande tillägg: "Myndigheten ska för varje informationssystem *som av myndigheten bedöms vara verksamhetskritiskt* dokumentera…"

Ett förtydliga önskas avseende vad som avses med produktionsmiljö, till exempel vad gäller forskningsapplikationer.

3 kap. Utveckling och anskaffning av informationssystem

Kravställning och kontroll 1-6§§
SLU bedömer att det krävs orimliga insatser för att uppfylla kravet när det handlar om forskningsverksamhet

3§2 innehåller flera bra punkter där SLU tolkar det som att det inte är ett skall-krav men att man i ex. systemdokumentationen visar att man tänkt på detta.

3§4 En avgränsning av kravet önskas genom följande tillägg: "Myndigheten ska för varje informationssystem som av myndigheten bedöms vara verksamhetskritiskt dokumentera…"

4 kap. Drift och förvaltning av informationssystem

Behörigheter, identiteter och autentisering 3-10§§
Ett förtydliga önskas avseende vad som avses med produktionsmiljö.

Internationella forskningsutbyten förekommer och som medför att informations-system på utomeuropeiska språk används, vilket bland annat omöjliggör att IT-säkerhetskraven säkerställs innan implementering.

Ändringshantering och uppdatering av programvara 17-21§§
Synpunkterna ovan om produktionsmiljö och internationella forskningsutbyten är tillämpliga även här.

Vidare ska myndigheten enligt de föreslagna föreskrifterna endast tillåta att på förhand godkända programvaror installeras och exekveras i myndighetens produktionsmiljö. Detta bedömer SLU kommer att bli svårt att upprätthålla i praktiken på grund av hur arbetet fungerar vid ett lärosäte. Avgörande för verksamheten är dels omfattande samarbeten där enskilda universitet inte själva styr vad som ska användas som samarbetsplattform. SLU bedömer att det skulle krävas en orimligt stor organisation för att kontrollera efterlevnaden.

Specifika synpunkter på förslaget om informationssäkerhet för statliga myndigheter

3§ Rubriken ”Begreppsförklaring” bör bytas till ”Definitioner”.

6§ Bestämmelsen syftar endast på när en myndighet överlåter till annan myndighet att utföra uppgifter enligt denna författning, det finns ett behov av att reglera vad som ska gälla när en myndighet uppdrar åt annan myndighet att ta fram information i egenskap av t.ex. expertkompetens. Ska ansvaret för att

informationsklassa informationen då ligga hos den myndighet som ger uppdraget eller den myndighet som utför uppdraget?

10§ Myndigheten ska ha ett dokumenterat arbetssätt för sitt informations-säkerhetsarbete som stöd för att

1. klassa information avseende konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få (informations-klassning),

Meningen kan förtydligas språkligt för att underlätta förståelsen för bestämmelsen. Vi föreslår följande skrivning: "Klassa vikten av informationens konfidentialitet, riktighet och tillgänglighet utifrån vilka konsekvenser ett bristande skydd kan få (informationsklassning)".

Eventuellt kan man specificera att konsekvenserna i detta fall ska syfta på konsekvenserna för myndigheten eller samhället.

11§ Positivt att begreppet "säkerställa" används.

Beslut om detta yttrande har universitetsdirektör Martin Melkersson fattat efter föredragning av chef för avdelningen för service, säkerhet och miljö (SSM) Per-Olov Skatt. Innehållet har utarbetats av informationssäkerhetsansvarig Christian Nähl och verksamhetskoordinator Agneta Höjdestrand vid avdelningen för service, säkerhet och miljö, IT-direktör Petra Lagerqvist, enhetschef Jan Bäckström samt IT-säkerhetsansvarig Pär Igsell vid IT-avdelningen samt universitetsjurist Erik Stavegren vid juridiska enheten.

Martin Melkersson

Per-Olov Skatt