En granskningsrapport från Riksrevisionen

Informationssäkerhet vid universitet och högskolor

– hanteringen av skyddsvärda forskningsdata

RiR 2023:20

RIKSREVISIONEN

Riksrevisionen är en myndighet under riksdagen med uppgift att granska statliga myndigheter och verksamheter. Vi bedriver både årlig revision och effektivitetsrevision. Genom ett grundlagsskyddat oberoende har Riksrevisionen ett starkt mandat och är en viktig del av riksdagens kontrollmakt som bidrar till förbättringar och demokratisk insyn.

Denna rapport har tagits fram inom effektivitetsrevisionen, vars uppgift är att granska hur effektiv den statliga verksamheten är. Vi lämnar även rekommendationer för att förbättra den granskade verksamheten. Effektivitetsgranskningar lämnas direkt till riksdagen som bereder dem tillsammans med en svarsskrivelse från regeringen.

Riksrevisionen

RiR 2023:20
ISBN 978-91-7086-671-5
ISSN 1652-6597
Omslagets originalfoto: Maskot Bildbyrå
Tryck: Riksdagstryckeriet, Stockholm 2023

Beslutad: 2023-11-23
Diarienummer: 2022/0652
RiR 2023:20

Till: Riksdagen

Härmed överlämnas enligt 9 § lagen (2002:1022) om revision av statlig verksamhet m.m. följande granskningsrapport:

Informationssäkerhet vid universitet och högskolor

– hanteringen av skyddsvärda forskningsdata

Riksrevisionen har granskat om universitet och högskolor bedriver ett effektivt informationssäkerhetsarbete för att hantera skyddsvärda forskningsdata. Resultatet av granskningen redovisas i denna granskningsrapport. Den innehåller slutsatser och rekommendationer som avser regeringen och 24 universitet och högskolor enligt nedan.

Riksrevisor Helena Lindberg har beslutat i detta ärende. Revisionsdirektör Sara Monaco har varit föredragande. Revisor Ludvig Stendahl, revisor Klara Folkesson och enhetschef Katarina Richardson har medverkat i den slutliga handläggningen.

Helena Lindberg

Sara Monaco

För kännedom

Regeringskansliet; Försvarsdepartementet, Utbildningsdepartementet

Universitet och högskolor enligt sändlista

Riksrevisionen

Sändlista

Blekinge tekniska högskola
Försvarshögskolan
Göteborgs universitet
Högskolan Dalarna
Högskolan i Borås
Högskolan i Gävle
Högskolan i Halmstad
Högskolan i Skövde
Högskolan Kristianstad
Högskolan Väst
Karlstads universitet
Kungl. Tekniska högskolan
Linköpings universitet
Linnéuniversitetet
Luleå tekniska universitet
Lunds universitet
Malmö universitet
Mittuniversitetet
Mälardalens universitet
Stockholms universitet
Södertörns högskola
Umeå universitet
Uppsala universitet
Örebro universitet

Innehåll

Elektroniska bilagor
Till rapporten finns bilagor i pdf-format att ladda ner från Riksrevisionens webbplats. Bilagorna kan även begäras ut från ärendets akt genom registraturen.

Sammanfattning

Målet för forskningspolitiken är att Sverige ska vara ett av världens främsta forsknings- och innovationsländer och en ledande kunskapsnation. Internationalisering och ett öppet vetenskapssamhälle ses som medel för att främja kvaliteten. Samtidigt behöver viss forskning skyddas för att inte skada exempelvis individers integritet, Sveriges konkurrenskraft eller samhällets säkerhet. Antalet cyberattacker har ökat och underrättelseverksamheten mot universitet och högskolor har intensifierats under senare år. Behovet av att lärosätena bedriver ett effektivt informationssäkerhetsarbete har därmed ökat.

Riksrevisionens övergripande slutsats är att lärosätena inte bedriver ett effektivt informationssäkerhetsarbete för att skydda forskningsdata. Trots att föreskriftskrav funnits sedan 2008 och bristerna varit kända sedan länge saknas fortfarande väsentliga delar av ett systematiskt informationssäkerhetsarbete. De åtgärder som regering, lärosäten och andra berörda myndigheter hittills vidtagit har inte varit tillräckliga.

Granskningen omfattar de 24 lärosäten som bedriver naturvetenskaplig och teknisk forskning.

Lärosätena arbetar inte effektivt för att identifiera skyddsvärda forskningsdata

Det är få forskare som klassar sina forskningsdata i enlighet med lärosätenas modeller för informationsklassning. Istället är det vanligt att externa finansiärer eller samarbetspartner ställer krav på att forskningsdata klassas, eller så gör forskarna en mindre formaliserad bedömning som inte dokumenteras. Den bristande systematiken i hur lärosätena identifierar skyddsvärda forskningsdata leder till att de saknar tillräckligt underlag för att bedöma risker och vilka skyddsåtgärder som är ändamålsenliga. Det kan också leda till att vissa skyddsvärda forskningsdata inte identifieras alls. Vidare förekommer det att forskare och institutioner har egna it-lösningar utanför den it-struktur som lärosätet tillhandahåller. Det kan innebära att skyddsvärda forskningsdata inte får ett ändamålsenligt skydd.

Lärosätena har otillräcklig kunskap och kompetens att bedöma vad som är skyddsvärt

Kunskap och kompetens i frågor kopplade till informationssäkerhet är överlag bristfälliga hos många medarbetare på lärosätena. Det gäller såväl kunskap om hur man praktiskt ska arbeta för att skydda sin information, som kunskap om hur man klassar sina forskningsdata och förhåller sig till gällande regelverk och externa krav. Lärosätena efterfrågar själva stöd för att bedöma externa hot och antagonister som kan utgöra informationssäkerhetsrisker. Granskningen visar att lärosätena gör olika bedömningar av vad som är skyddsvärt, vilket kan leda till att skyddsvärda forskningsdata inte får ett ändamålsenligt skydd. De utbildningar som lärosätena erbjuder når ett fåtal medarbetare. Lärosätena har också utmaningar att rekrytera och behålla kompetens inom området.

Lärosätesledningarna har inte styrt och organiserat informationssäkerhetsarbetet på ett effektivt sätt

Lärosätesledningarna har inte sett till att beslutade riktlinjer, rutiner och arbetssätt implementeras i hela organisationen. Det finns otydligheter i roll- och ansvarsfördelning på olika nivåer inom lärosätena. Till exempel är både prefekter och forskare osäkra på vilket ansvar de har för informationssäkerhet och vad det innebär i praktiken. Det stöd som lärosätena tillhandahåller för att hantera forskningsdata har begränsat genomslag. Stödet är heller inte alltid samordnat med informationssäkerhetsfunktionerna vid lärosätet. De som är utsedda att samordna och leda informationssäkerhetsarbetet saknar ofta förutsättningar att bedriva ett strategiskt arbete, bland annat på grund av sin organisatoriska placering. De rapporterar inte heller alltid regelbundet till rektor eller styrelse.

Regeringens och myndigheternas åtgärder för att stärka informationssäkerhetsarbetet har varit otillräckliga

Trots kännedom om att lärosätena under en längre tid haft brister i sitt arbete kopplat till informationssäkerhet var det först 2019 som regeringen började följa upp arbetet mer systematiskt genom myndighetsdialoger och olika återrapporteringskrav. Myndigheten för samhällsskydd och beredskaps utbildningsinsatser, metodstöd och verktyg för uppföljning av det systematiska informationssäkerhetsarbetet har inte haft tillräckligt genomslag i högskolesektorn. Detsamma gäller exempelvis Säkerhetspolisens och Inspektionen för strategiska produkters utbildningsinsatser riktade till lärosätena.

Rekommendationer

Till regeringen

- Ge uppdrag till Myndigheten för samhällsskydd och beredskap att genomföra kompetenshöjande insatser till ledningarna för universitet och högskolor. Insatserna bör anpassas efter lärosätenas behov.
- Ge uppdrag till universitet och högskolor att i samverkan inrätta en gemensam stödfunktion för informationssäkerhet. Etableringen bör ske i samråd med Myndigheten för samhällsskydd och beredskap och andra relevanta myndigheter. Dessa myndigheter bör även ge råd och stöd efter att funktionen etablerats. Stödfunktionen ska kunna bistå universitet och högskolor med bland annat följande:
    - rådgivning till dem som leder och samordnar informationssäkerhetsarbetet om bland annat utformning av informationssäkerhetsarbetet, analys, säkerhetsåtgärder samt tolkning och efterlevnad av regelverk om till exempel säkerhetsskydd och exportkontroll
    - behovsanpassade utbildningar och kurser i informationssäkerhet för samtliga medarbetare vid lärosätena
    - stöd för att analysera och bedöma sektorsgemensamma risker och externa hot till relevanta funktioner på lärosätena.

Stödfunktionen kan med fördel dra nytta av kunskap och erfarenheter från bland annat pågående lärosätesgemensamma samarbeten och nätverk inom informationssäkerhetsområdet.

Till de 24 universitet och högskolor som ingår i granskningen

- Se till att roller och ansvarsfördelning är tydliga från ledningsnivå till enskilda medarbetare, så att varje medarbetare vet sitt ansvar när det gäller att hantera forskningsdata korrekt.
- Se till att de som leder det strategiska informationssäkerhetsarbetet har mandat att ställa krav och granska informationssäkerhetsarbetet samt att de regelbundet rapporterar till lärosätesledning och styrelse.
- Se till att arbetssätten för informationsklassning av forskningsdata är enhetliga.
- Se till att det finns kompetens att analysera informationssäkerhetsrisker kopplade till forskningsdata.
- Se till att det finns ett samordnat stöd för medarbetare att hantera forskningsdata korrekt under hela livscykeln.

1 Inledning

1.1 Motiv till granskning

Målet med forskningspolitiken är att Sverige ska vara ett av världens främsta forsknings- och innovationsländer och en ledande kunskapsnation.[1] Sverige är ett av de länder i världen som gör störst investeringar i forskning och utveckling (FoU), över 3 procent av BNP 2022.[2] Syftet är bland annat att skapa arbetstillfällen, tillväxt och konkurrenskraft.[3] En stor del av forskningen bedrivs vid universitet och högskolor; 2022 uppgick de totala utgifterna för egen FoU vid universitet och högskolor till drygt 44 miljarder kronor.[4]

Många länder eftersträvar den innovationskraft och kunskapsintensitet som Sverige står för och kontakter med svenska lärosäten ses som en väg till att ta del av det svenska innovationssystemet.[5] Antalet cyberattacker har ökat och underrättelseverksamheten mot universitet och högskolor har intensifierats under senare år.[6] Teknik- och kunskapsanskaffning är prioriterat för främmande makt i syfte att bland annat gynna det egna landets konkurrenskraft och militära förmåga.[7] Mörkertalet är stort men Säkerhetspolisen uppskattar att det stjäls information och kunskap till ett värde av miljardbelopp varje år.[8] Utbildningsutskottet har uttalat att det är viktigt att Sverige har en god förmåga att skydda bland annat forskning från industrispionage och att det är viktigt att följa dessa frågor för att bedöma om ytterligare åtgärder behövs.[9]

En övervägande del av forskningen och forskningsdata[10] kan vara öppen och tillgänglig för alla. Men vissa forskningsdata är skyddsvärda eftersom de rör exempelvis personuppgifter, företagshemligheter eller säkerhetskänslig verksamhet.

---

1 Prop. 2016/17:50, s. 20, bet. 2016/17:UbU12, rskr. 2016/17:208.
2 SCB, ”Ökad FoU-verksamhet i Sverige under 2022”, hämtad 2023-11-13.
3 Prop. 2020/21:60, s. 13–14, bet. 2020/21:UbU16, rskr. 2020/21:254.
4 SCB, ”Totala utgifter för egen FoU-verksamhet efter sektor, typ av utgift och år, 2022”, hämtad 2023-11-14.
5 SOU 2018:3, s. 78–80.
6 TT, ”Säpo: Underrättelsehoten mot lärosäten ökar”, 2021-05-21; Hellerstedt, ”Spioneriet mot svenska lärosäten fortsätter öka”, 2023-03-09; SVT, ”Attacker mot svenska universitets hemsidor”, 2023-02-11.
7 Se t.ex. Olsson, *Cyberattacker mot universitet ökar*, 2021-10-07; intervju med företrädare för Säkerhetspolisen, 2023-03-24 och 2022-10-20.
8 Säkerhetspolisen, *Säkerhetspolisen 2020*, 2021, s. 24; mejl från företrädare för Säkerhetspolisen, 2022-11-25.
9 Prop. 2020/21:60, bet. 2020/21:UbU16, s. 38, rskr. 2020/21:254.
10 Forskningsdata avser data som samlas in eller framställs inom ramen för vetenskaplig forskningsverksamhet, se vidare Ordlista.

Sedan 2008 är alla statliga myndigheter, inklusive statliga universitet och högskolor, skyldiga att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.[11] Syftet är att ge information tillräckligt skydd utifrån dess värde.

Informationssäkerhet och skyddsvärda forskningsdata

Informationssäkerhet innebär bevarande av *konfidentialitet* (endast behöriga får ta del av informationen), *riktighet* (att informationen inte är manipulerad) och *tillgänglighet* (att informationen finns när behörig efterfrågar den) hos information utifrån dess värde.[12]

Konfidentialitet är resultatet av en bedömning, ibland med stöd i lagar och andra krav.[13] Kraven på konfidentialitet grundar sig bland annat på bestämmelser om sekretess, dataskydd och t.ex. säkerhetsskyddslagstiftningen. Konfidentialiteten kan förändras över tid.

Med **skyddsvärda forskningsdata** avses i den här granskningen i första hand sådana data som behöver skyddas på grund av sekretess, dataskyddsreglering eller annan specialreglering, se vidare kapitel 2. Det kan exempelvis röra stora mängder eller känsliga personuppgifter, företagshemligheter eller säkerhetskänslig verksamhet.

Regeringen har på olika sätt sedan 2019 haft frågan om säkerhet på universitet och högskolor på dagordningen, bland annat i myndighetsdialoger, regleringsbrev och utredningsuppdrag.[14] Det finns sedan länge en politisk målsättning om ett öppet vetenskapssamhälle med fri tillgång till vetenskapliga texter, forskningsresultat och forskningsdata.[15] I den senaste forskningspropositionen beskriver regeringen att internationell samverkan och en hög grad av internationalisering är en

11 6 § MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6). Se avsnitt 2.2 för en beskrivning av de föreskrifter som gällde innan dess.

12 3 § MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6); MSB:s metodstöd för systematiskt informationssäkerhetsarbete, informationssäkerhet.se, ”Klassningsmodell”, hämtad 2023-05-05.

13 MSB, ”Termbanken för informationssäkerhet”, hämtad 2023-11-11.

14 Regeringskansliet, Utbildningsdepartementet, Dagordningar för myndighetsdialoger med Blekinge tekniska högskola, KTH och Lunds universitet 2019–2022, se referenslista. I lärosätenas regleringsbrev för 2022 och 2023 finns återrapporteringskrav rörande arbetet med informationssäkerhet, se regeringsbeslut U2021/04851 (delvis), U2021/04891; regeringsbeslut U2022/02763, U2022/02805, U2022/02810 m.fl. Se också Regeringskansliet, U2020/03059/UH, 2020-05-06; Regeringskansliet, U2023/02485, 2023-08-31; Utbildningsdepartementet, ”Pressmeddelande: Nya styrelser för 30 universitet och högskolor”, 2023-04-27.

15 Se t.ex. prop. 2012/13:30, s. 150–152, bet. 2012/13:UbU3, rskr. 2012/13:51; prop. 2016/17:50, s. 106, bet 2016/17:UbU12, rskr. 2016/17:208; prop. 2020/21:60, s. 100, bet. 2020/21:UbU16, rskr. 2020/21:254.

förutsättning för att Sverige ska vara en ledande forsknings- och kunskapsnation. Men regeringen menar också att internationella forskningssamarbeten kan innebära vissa risker och ser därför behov att säkerställa skydd av forskningsresultat.[16]

Riksrevisionen granskade det interna styrningen och kontrollen av informationssäkerheten vid universitet och högskolor 2009 och 2010. Sammanfattningsvis konstaterades stora brister gällande bland annat roll- och ansvarsfördelning, riskanalys inklusive informationsklassning samt avsaknad av styrdokument.[17] Genom åren har internrevisionen vid många lärosäten genomfört granskningar som visar på fortsatta brister.[18] Mycket tyder på att informationssäkerhetsarbetet vid lärosätena fortsatt är på en generellt låg nivå och att de har bristande kunskap om vad som är skyddsvärt.[19] Myndigheten för samhällsskydd och beredskap (MSB) konstaterar att arbetet med systematisk informationssäkerhet är eftersatt hos majoriteten av de statliga myndigheterna.[20] Men jämfört med andra branscher uppvisar högskolesektorn lägre engagemang för informationssäkerhet.[21]

Det förändrade säkerhetshetspolitiska läget har satt ytterligare fokus på riskerna med lärosätenas bristande informationssäkerhetsarbete. Riksrevisionen har mot bakgrund av detta samt sektorns komplexitet med många uppdrag och mål återigen granskat lärosätenas arbete med informationssäkerhet. Genom att analysera även

16 Prop. 2020/21:60, s. 27, bet. 2020/21:UbU16, rskr. 2020/21:254.

17 De lärosäten som granskades 2010 (avseende 2009) var: Blekinge tekniska högskola, Högskolan i Borås, Högskolan i Halmstad, Högskolan Kristianstad, Högskolan i Skövde, Linköpings universitet, Lunds universitet och Sveriges lantbruksuniversitet. 2011 granskades följande lärosäten (avseende 2010): Gymnastik- och idrottshögskolan, Högskolan i Gävle, Karolinska institutet, Konstfack, Kungl. Konsthögskolan, Kungl. Musikhögskolan i Stockholm samt Mälardalens högskola (sedan 2022 universitet). 2012 granskades Malmö högskola (sedan 2018 universitet) avseende 2011. Samtliga rapporter finns att hämta på riksrevisionen.se.

18 Till exempel KTH, Internrevisionen, *Granskning av KTH:s ledningssystem för informationssäkerhet, Revisionsrapport 1/2020,* 2020-10-01; Malmö universitet, Internrevisionen, *Granskning av IT-säkerhetskultur vid Malmö universitet*, 2022-12-01; PwC, Stockholms universitet, *Granskning av informationssäkerhet*, november 2020; Lunds universitet, Internrevisionen, *Granskning av cyber- och informationssäkerhet*, 2019-12-13; Uppsala universitet, Internrevisionsrapport, *Informationssäkerhetsarbete*, 2021-12-14; PwC, Luleå tekniska universitet, Internrevision 2021, *Informationssäkerhet*, 2021-04-21.

19 Genomgång av underlag till MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen, Resultatredovisning Infosäkkollen 2021*, 2022b, 2022-08-26. Av de 15 svarande lärosätena är det endast ett fåtal som har grunderna i informationssäkerhet på plats, och inget lärosäte lever upp till MSB:s föreskriftskrav. Se också SOU 2021:97, enkätsvar från 12 lärosäten; Säkerhetspolisen, *Säkerhetspolisen 2020*, 2021, s. 40.

20 MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen, Resultatredovisning Infosäkkollen 2021*, 2022b, s. 17.

21 Hallberg, m.fl. (red.), *Informationssäkerhet och organisationskultur,* 2017, s. 50–51.

orsakerna till de brister som konstateras bidrar granskningen med underlag för ett effektivare informationssäkerhetsarbete på universitet och högskolor och ytterst ett bättre skydd för den information som behöver skyddas.

1.2 Övergripande revisionsfråga och avgränsningar

Den övergripande revisionsfrågan är om universitet och högskolor bedriver ett effektivt informationssäkerhetsarbete som möjliggör att skyddsvärda forskningsdata hanteras säkert och enligt gällande regelverk. Med effektivt avses att informationssäkerhetsarbetet bedrivs systematiskt och riskbaserat.[22]

För att besvara den övergripande frågan ställer vi två delfrågor:

1. Arbetar universitet och högskolor effektivt för att identifiera skyddsvärda forskningsdata och analysera informationssäkerhetsrisker?
2. Har universitet och högskolor utformat informationssäkerhetsarbetet på ett effektivt sätt för att hantera skyddsvärda forskningsdata?

Granskningen omfattar regeringen och de 24 statliga universitet och högskolor som bedriver teknisk och naturvetenskaplig forskning, se vidare avsnitt 1.4 och bilaga 1.

Informationssäkerhet täcker in all information som en organisation hanterar. I granskningen fokuserar vi på forskningsdata. Rutiner, riktlinjer och arbetssätt i informationssäkerhetsarbetet kan dock förstås inkludera annan information än forskningsdata. Vi fokuserar på den organisatoriska säkerheten i lärosätenas informationssäkerhetsarbete.[23] Det är framför allt inom denna del som vi har tagit del av problemindikatorer. Frågan om huruvida forskningsdata faktiskt skyddas ligger utanför granskningen.

1.3 Bedömningsgrunder

Bedömningsgrunder är de kriterier som Riksrevisionen tillämpar för att värdera sina iakttagelser. I det här avsnittet går vi igenom de övergripande bedömningsgrunderna och därefter hur vi har operationaliserat dem kopplat till det två delfrågorna.

---

22 Med systematiskt avses att arbeta strukturerat efter en bestämd process med analys, utformande och genomförande, samt uppföljning, utvärdering och förbättring. Att arbeta riskbaserat innebär att identifiera de risker som hänger samman med den information som verksamheten hanterar och anpassa skyddet av informationen utifrån denna analys. I granskningen har vi fokuserat på analys, utformande och genomförande. Se vidare avsnitt 2.1.1.

23 Informationssäkerhet kan delas upp i organisatoriska, personrelaterade, fysiska och tekniska säkerhetsåtgärder, se vidare kapitel 2 och Ordlista.

En övergripande utgångspunkt i granskningen är högskolelagen (1992:1434) där det framgår att lärosätena ska verka för att den kunskap och kompetens som finns vid högskolan kommer samhället till nytta och att den samlade internationella verksamheten vid varje högskola ska stärka kvaliteten i högskolans utbildning och forskning.[24] Av högskoleförordningen (1993:100) framgår att det ska finnas finns en intern styrning och kontroll som fungerar på ett betryggande sätt.[25] Vidare gäller att myndigheter ska verka för att genom samarbete med myndigheter och andra ta till vara fördelar som kan finnas för enskilda och staten som helhet.[26]

I propositionen 2020/21:1 understryker regeringen att styrningen av statsförvaltningen ska vara långsiktig, strategisk, helhetsinriktad, sammanhållen, verksamhetsanpassad och tillitsbaserad. Detaljstyrning och onödig administration ska undvikas. Det förutsätter att regeringen följer upp myndigheternas resultat och verksamhet och ingriper om den bedömer att myndigheterna inte sköter sina uppgifter på ett ändamålsenligt sätt.[27]

I propositionen 2001/02:158, *Samhällets säkerhet och beredskap*, presenterade regeringen en ansvarsfördelning mellan myndigheter för informationssäkerhetsarbetet i samhället.[28] MSB har i uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet.[29]

Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (upphörde gälla oktober 2022) och efterföljande förordning (2022:524) om statliga myndigheters beredskap reglerar bland annat informationssäkerhetsarbetet för myndigheter under regeringen. Här framgår att varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. I ansvaret ingår att

24 1 kap. 2 och 5 §§ högskolelagen (1992:1434).

25 2 kap. 2 § första stycket 2 högskoleförordningen (1993:100). För 15 högskolor finns också krav på att tillämpa internrevisionsförordningen (2006:1228), se 1 kap. 5 a § högskoleförordningen (1993:100).

26 6 § myndighetsförordningen (2007:515).

27 Prop. 2020/21:1, utg.omr. 2, s. 58, bet. 2020/21:FiU2, rskr. 2020/21:150.

28 Prop. 2001/02:158, bet. 2001/02:FÖU10, s. 72, rskr. 2001/02:261.

29 11 a § förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

myndigheten särskilt ska beakta behovet av säkra ledningssystem.[30] Förordningen bemyndigar MSB att meddela föreskrifter om informationssäkerhet.[31]

ISO 27000-standarden utgör en internationell standard för ledningssystem för informationssäkerhet (LIS) som ett sätt att styra en verksamhets informationssäkerhet på ett systematiskt sätt.[32] Av MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) framgår att myndigheterna ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av dessa standarder.[33]

I MSB:s föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7) preciseras vilka tekniska åtgärder som krävs. I MSB:s föreskrifter om rapportering av it-incidenter för statliga myndigheter (MSBFS 2020:8) preciseras bestämmelser om rapportering av it-incidenter.

På uppdrag av regeringen har MSB utformat ett metodstöd för att stödja arbetet att implementera ett systematiskt informationssäkerhetsarbete i enlighet med föreskrifterna. Metodstödet utgår från ISO-27000 serien.[34] (Se även kapitel 2 om MSB:s metodstöd.) Utifrån ovanstående utgångspunkter har vi operationaliserat bedömningsgrunderna för respektive delfråga.

1.3.1 Operationaliserade bedömningsgrunder för delfråga 1

Informationssäkerhetsarbetet ska omfatta all behandling av information som myndigheten ansvarar för.[35] Informationsklassning och riskbedömning är centrala delar i ett systematiskt informationssäkerhetsarbete. Informationsklassning innebär att identifiera information och värdera dess värde och känslighet.[36]

Enligt Riksrevisionen är genomförd informationsklassning och riskbedömning viktiga förutsättningar för att en organisation ska kunna identifiera behov av och vidta ändamålsenliga säkerhetsåtgärder. En för låg klassning riskerar att leda till

---

30 13 § förordningen (2022:524) om statliga myndigheters beredskap. För Försvarshögskolan gäller inte bestämmelserna i 12 § andra stycket om informationsskyldighet, 14 § om it-incidentrapportering och 17 § om risk- och sårbarhetsbedömning.

31 26–27 §§ förordningen (2022:524) om statliga myndigheters beredskap. MSB:s mandat är överflyttat i oförändrad form till den nya förordningen, mejl från företrädare för MSB, 2023-09-26.

32 Se bl.a. Svenska institutet för standarder, Svensk standard SS-EN ISO/IEC 27000:2020 *Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Översikt och terminologi (ISO/IEC 27000:2018)*, utgåva 2.

33 4 § MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

34 Se MSB:s metodstöd för systematiskt informationssäkerhetsarbete, informationssäkerhet.se, ”Metodstöd”, hämtad 2023-03-21.

35 5 § MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

36 MSB och Riksarkivet, *Vägledning för processorienterad informationskartläggning*, 2012, s. 33.

otillräckliga åtgärder och därmed verksamhetsrisker, medan en för hög klassning kan leda till överflödiga åtgärder med onödig administration och högre kostnader som följd. En systematisk informationsklassning och riskbedömning är alltså en förutsättning för att kunna vidta proportionella och ändamålsenliga säkerhetsåtgärder.

Riksrevisionen har formulerat följande villkor som behöver vara uppfyllda för att vi ska bedöma att universitet och högskolor arbetar effektivt för att identifiera skyddsvärda forskningsdata.

- Forskningsdata ska inventeras och klassificeras utifrån skyddsvärde och skyddsbehov. Det ska göras systematiskt utifrån vilka konsekvenser ett bristande skydd kan få. Genom att använda en gemensam klassningsmodell kan organisationens information skyddas på ett enhetligt sätt utifrån interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet. Klassningsmodellen ska vara enkel att använda. Ledningen behöver se till att implementera ett arbetssätt som är ändamålsenligt och fungerar i praktiken.
- Lärosätena ska identifiera, analysera och värdera riskerna för sina forskningsdata. Det ska finnas processer som fångar upp identifierade risker på olika relevanta nivåer och en systematik som möjliggör återkommande uppföljning. För att upprätta en bra riskanalys krävs underlag i form av bland annat informationsklassning, rapporterade it-incidenter och uppföljning. Medarbetare ska veta vad en informationssäkerhetsincident är och hur den ska rapporteras. Arbetet med riskanalyser ska involvera funktioner från relevanta delar av verksamheten.

1.3.2 Operationaliserade bedömningsgrunder för delfråga 2

För att kunna bedriva ett effektivt informationssäkerhetsarbete behöver det finnas processer och strukturer som styr arbetet och möjliggör en säker hantering av information. Riksrevisionen har formulerat följande villkor som behöver vara uppfyllda för att vi ska bedöma att universitet och högskolor har utformat informationssäkerhetsarbetet på ett effektivt sätt för att hantera skyddsvärda forskningsdata:

- Det ska finnas en policy för informationssäkerhetsarbetet där ledningens mål och inriktning för informationssäkerhetsarbetet tydligt framgår. Ledningen har det yttersta ansvaret för att styra och organisera verksamheten så att den fungerar effektivt i enlighet med uppställda mål. Det inkluderar att avsätta tillräckliga resurser för informationssäkerhetsarbetet. Det innebär att

lärosätena behöver budgetera utifrån den omfattning som krävs för att bedriva ett effektivt informationssäkerhetsarbete. Ledningen ska också hålla sig informerad om informationssäkerhetsläget, både löpande och vid särskilda genomgångar med den eller de som leder och samordnar informationssäkerhetsarbetet.

- Roll- och ansvarsfördelning för informationssäkerhetsarbetet ska tydligt framgå av styrdokument och riktlinjer. Det ska vara tydligt för dem med utpekat ansvar vad ansvaret innebär och vilket mandat som följer med. Den eller de som utses att leda och samordna informationssäkerhetsarbetet ska ha mandat att ställa krav och granska samt rapportera direkt till ledningen.
- För att säkerställa att information hanteras på ett säkert sätt behöver lärosätets medarbetare och inhyrd personal ha kompetens inom informationssäkerhet som är relevant och anpassad till funktion. Kompetensen ska utvecklas och upprätthållas genom utbildning, informationsinsatser och övning. Alla i organisationen ska känna till relevanta styrdokument, regelverk och arbetssätt och därigenom förstå sin roll och sitt ansvar. Beroende på vilken information medarbetare ska få åtkomst till, behöver lärosätet anpassa sin bakgrundskontroll.
- Det ska finnas lätt tillgängligt och verksamhetsanpassat stöd för att hantera forskningsdata. Stödet ska vara samordnat efter behov och möjliggöra en säker hantering av forskningsdata i enlighet med gällande rättsliga krav.

1.4 Metod och genomförande

Vi har använt oss av en kombination av intervjuer, dokumentstudier och en enkät. Granskningen omfattar 24 lärosäten, varav 3 är valda som exempel på hur olika typer av lärosäten kan arbeta med informationssäkerhet. Syftet är inte bara att uttala oss om exempellärosätena, utan att genom iakttagelser från dem kunna dra slutsatser som kan vara relevanta för hela sektorn. En utförlig beskrivning av metod finns i bilaga 1.

En vägledande princip i urvalet har varit att fånga så mycket variation som möjligt bland annat i organisationsstruktur, storlek, finansieringsformer och forskningsämnen. Det gäller för såväl lärosäten som institutioner och funktioner inom dessa lärosäten. En översiktlig beskrivning av exempellärosätena finns i bilaga 3.

Vi har genomfört 65 intervjuer vid de 3 exempellärosätena Blekinge tekniska högskola, Kungl. Tekniska högskolan och Lunds universitet, se bilaga 2. Vid

respektive lärosäte har vi intervjuat forskare, prefekter, dekaner eller motsvarande, förvaltningschef och informationssäkerhetschef eller informationssäkerhetsansvarig. Vi har också intervjuat roller och funktioner inom bland annat it och it-säkerhet, säkerhet och säkerhetsskydd, juridik, forskningsdatahantering, exportkontroll och dataskydd. Därutöver har vi gjort intervjuer bland annat vid Malmö universitet, Sveriges lantbruksuniversitet och RISE Research Institutes of Sweden AB som del av inledande informationsinhämtning.

Vi har även intervjuat företrädare för Säkerhetspolisen, MSB, Vetenskapsrådet samt länsstyrelserna Norrbotten, Skåne, Stockholm och Västra Götaland. Utöver det har vi intervjuat andra aktörer med relevant kunskap för granskningen, se vidare bilaga 1.

Vi har tagit del av och analyserat styrdokument och annan dokumentation från de tre exempellärosätena såsom informationssäkerhetspolicyer, delegationsordningar, interna beslut och riskanalyser. Utöver det har vi tagit del av en rad olika dokument, exempelvis utredningar, propositioner och rapporter.

Enkäten bestod av två delar där den första handlade brett om informationssäkerhet och den andra begränsades till frågor om säkerhetsskydd. Enkätens båda delar omfattar 24 lärosäten och genomfördes för att få en bredare bild av hur universitets- och högskolesektorn arbetar med informationssäkerhet gällande forskningsdata. Den inkluderade frågor om bland annat styrning, roll- och ansvarsfördelning, inventering och klassning av information, riskarbete, utbildning, resurser och säkerhetsskydd. Svarsfrekvensen var 100 procent. Enkätens båda delar återfinns i bilaga 4.

Granskningen har genomförts av en projektgrupp bestående av Sara Monaco (projektledare), Ludvig Stendahl och Klara Folkesson. Jens Pettersson deltog i granskningen till februari 2023 och Josefine Olsson till augusti 2023. Stina Lindgren (praktikant) och Lars Henning (revisor) har också bidragit i arbetet. En referensperson har lämnat synpunkter på granskningsupplägg och på ett utkast till granskningsrapport: Jonas Hallberg, tekn. dr, enhetschef Cyberförsvar, Totalförsvarets forskningsinstitut (FOI). Företrädare för Regeringskansliet (Försvarsdepartementet, Justitiedepartementet, Landsbygds- och infrastrukturdepartementet och Utbildningsdepartementet), Blekinge tekniska högskola, Kungl. Tekniska högskolan, Lunds universitet, Myndigheten för samhällsskydd och beredskap, Säkerhetspolisen och länsstyrelserna i Norrbotten, Skåne, Stockholm och Västra Götaland har fått tillfälle att faktagranska och i övrigt lämna synpunkter på ett utkast till granskningsrapport.

2 Om informationssäkerhet och lärosäten

I kapitlet går vi översiktligt igenom viktiga delar i ett systematiskt informationssäkerhetsarbete, Myndigheten för samhällsskydd och beredskaps (MSB) stöd och uppdrag inom området samt ett urval relevanta regelverk. Vi redogör kortfattat för regeringens styrning av statliga universitet och högskolor. Därefter går vi igenom lärosätenas interna styrning och organisation och huvudsakliga roller som vi bedömer är relevanta för informationssäkerhetsarbetet. Avslutningsvis beskriver vi regeringens styrning av lärosätena med koppling till säkerhet och informationssäkerhet samt målen om internationalisering och ett öppet vetenskapssamhälle.

2.1 Myndigheten för samhällsskydd och beredskaps stöd för ett systematiskt informationssäkerhetsarbete

MSB har ett utpekat ansvar att stödja och samordna arbetet med samhällets informationssäkerhet. Här ingår även att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och regioner samt företag och organisationer.[37]

2.1.1 Delar i ett systematiskt informationssäkerhetsarbete

Kärnan i informationssäkerhet handlar om att styra och skydda information utifrån aspekterna riktighet, tillgänglighet och konfidentialitet så att rätt person har tillgång till rätt information vid rätt tillfälle.[38] Ett systematiskt informationssäkerhetsarbete är ett arbetssätt för att identifiera krav på och införa säkerhetsåtgärder som ger tillräckligt skydd för informationen. MSB betonar i sitt metodstöd att det är byggt efter en idealiserad bild av hur arbetet kan bedrivas. I praktiken pågår ofta arbete inom flera områden samtidigt.[39]

---

37 11 a § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

38 Ibland läggs även spårbarhet till som en aspekt. Definitionen med dessa tre (eller fyra) aspekter har kritiserats bl.a. för att utgå från att dessa specifika villkor gäller för all information i alla sammanhang, se Hallberg, m.fl. (red.), 2017, s. 212–213.

39 Myndigheten för samhällsskydd och beredskaps metodstöd för systematiskt informationssäkerhetsarbete, informationssäkerhet.se, ”Metodstödet”, hämtad 2023-03-21.

Figur 1 De fyra metodstegen i MSB:s metodstöd utgör helheten av det systematiska informationssäkerhetsarbetet

Källa: MSB, Ledningens roll inom informationssäkerhet. Stöd för dig med en ledande funktion. Ledningens genomgång, 2021, s. 7.

I varje metodsteg finns ett antal underliggande delar. *Identifiera och analysera* består av verksamhetsanalys, omvärldsanalys, riskbild och gapanalys. Analyserna ska säkerställa att informationssäkerheten i verksamheten utformas med utgångspunkt i ett tydligt definierat nuläge.

Utforma är uppdelat i nio delar som behövs för verksamhetens systematiska informationssäkerhetsarbete: organisation, ledning och styrning, informationssäkerhetsmål, styrdokument, riskhantering, klassningsmodell, välj säkerhetsåtgärder[40] och skapa skyddsnivåer, handlingsplan, kontinuitetshantering för informationstillgångar samt incidenthantering.

När styrningen är utformad ska organisationen *använda* den genom följande delar: riskanalys, klassning av information, genomföra och efterleva samt utbilda och kommunicera.

Det sista steget *Följa upp och förbättra* består av delarna utvärdera och följa upp samt ledningens genomgång.

40 Säkerhetsåtgärder för informationssäkerhet omfattar åtgärder inom det organisatoriska, personrelaterade, tekniska och fysiska säkerhetsområdet. Åtgärderna kan verka förebyggande, upptäckande eller korrigerande, se vidare Ordlista.

2.1.2 MSB:s råd och stöd inom informationssäkerhet

MSB har haft ett särskilt uppdrag att genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor som redovisades i mars 2021.[41] Det har framför allt gjorts i form av utbildningar och utvecklat metodstöd (se ovan).[42] MSB har också haft i uppdrag att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.[43] I maj 2021 lanserades uppföljningsstrukturen under namnet Infosäkkollen, riktad till kommuner, regioner och statliga myndigheter. Genom frivilliga självvärderingar är syftet att vartannat år följa upp det systematiska informationssäkerhetsarbetet. Det finns också möjligheter för de inrapporterande organisationerna att på gruppnivå jämföra sina egna resultat med andra svarande organisationers.[44] 15 lärosäten besvarade den första Infosäkkollen.[45] Inför 2023 års rapportering har it-säkkollen lagts till med fokus på it-säkerhetsåtgärder.[46]

Sedan hösten 2022 erbjuder MSB en rådgivningstjänst om det systematiska informationssäkerhetsarbetet via mejl eller telefon som ett komplement till övriga vägledningar och stödmaterial.[47] MSB är också sammankallande för det statliga nätverket för informationssäkerhet (Snits). Nätverket syftar till kontakt- och erfarenhetsutbyte, kompetensutveckling, informationsspridning och diskussioner om systematiskt informationssäkerhetsarbete.[48]

2.2 Viktiga regelverk rörande informationssäkerhet och hanteringen av forskningsdata

Det finns ett antal regelverk som reglerar informationssäkerhet och hanteringen av forskningsdata. Nedan sammanfattar vi de generella regelverk som vi bedömer är mest relevanta för hanteringen av forskningsdata, varav en del är mer relevanta just

41 Regeringsbeslut Ju2019/03057/SSK. Under 2018 och 2019 riktade MSB utbildningsinsatser till kommuner, regioner och länsstyrelser.

42 År 2011 lanserade MSB det första metodstödet för systematiskt informationssäkerhetsarbete och en reviderad version lanserades 2018.

43 Regeringsbeslut Ju2019/03058/SSK, Ju2019/02421/SSK.

44 MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen, Resultatredovisning Infosäkkollen 2021*, 2022b, s. 17.

45 Genomgång av underlag till MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen, Resultatredovisning Infosäkkollen 2021*, 2022b, 2022-08-26.

46 MSB, ”Infosäkkollen”, hämtad 2023-10-09.

47 MSB, ”Rådgivningstjänst för systematiskt informationssäkerhetsarbete”, hämtad 2023-09-18.

48 MSB, ”Nätverk för offentliganställda”, hämtad 2023-10-03.

inom naturvetenskap och teknik. Det finns även många andra regelverk som kan vara aktuella utöver de som anges nedan och listan är inte uttömmande.[49]

Relevant rättslig reglering

Informationssäkerhet: förordningen (2022:524) om statliga myndigheters beredskap; Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6)[50]; Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7); Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av it-incidenter för statliga myndigheter (MSBFS 2020:8).

Personuppgifter: Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning); lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Tillsynsmyndighet: Integritetsskyddsmyndigheten.

Allmänna handlingars offentlighet och sekretess: 2 kap. tryckfrihetsförordningen; offentlighets- och sekretesslagen (2009:400)

Säkerhetsskydd: säkerhetsskyddslagen (2018:585); säkerhetsskyddsförordningen (2021:955); Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1).

Tillsynsmyndighet: sedan 2021 är länsstyrelserna i Norrbotten, Stockholm, Skåne och Västra Götaland tillsynsansvariga för universitet och högskolor beroende på var lärosätet har sitt säte.[51]

---

49 Exempelvis lagen (2018:558) om företagshemligheter; lagen (2003:460) om etikprövning av forskning som avser människor, lagen (1984:3) om kärnteknisk verksamhet och lagen (2002:297) om biobanker i hälso- och sjukvården m.m. Listan kan göras betydligt längre och tillämpliga regelverk kan variera mellan forskningsområden.

50 Innan dessa gällde MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1), som ersatte MSBFS 2009:10 föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet, som i sin tur ersatte Verket för förvaltningsutvecklings föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte (VERVAFS 2007:2). Föreskriften trädde i kraft 2008 med krav på att myndigheter under regeringen skulle tillämpa ett ledningssystem för informationssäkerhet. MSB, *Konsekvensutredning för föreskrift om krav på informationssäkerhet*, 2009-11-24.

51 Se 8 kap. 1 § säkerhetsskyddsförordningen (2021:955). Försvarsmakten är tillsynsmyndighet för Försvarshögskolan.

Arkivering och gallring[52]**:** arkivlagen (1990:782); arkivförordningen (1991:446); Riksarkivets föreskrifter och allmänna råd om gallring av handlingar i statliga myndigheters forskningsverksamhet (RA-FS 1999:1).

Tillsynsmyndighet: Riksarkivet

Exportkontroll och produkter för civil användning som även kan användas militärt: lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd; förordningen (2000:1217) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd.

Tillsynsmyndighet: Inspektionen för strategiska produkter.

2.3 Regeringens styrning av statliga lärosäten

Högskolesektorn i Sverige[53]

År 2022 fanns det 16 statliga universitet och 15 statliga högskolor i Sverige samt ett tjugotal enskilda utbildningsanordnare[54]. Sammanlagt fanns 55 000 heltidsekvivalenter (motsvarande ca 69 000 anställda varav 55 procent var kvinnor och 45 procent män). Av dessa var drygt 32 000 forskande och undervisande personal. Vidare fanns drygt 17 000 doktorander (varav kvinnor 52 procent och män 48 procent) och 370 000 studenter (varav 61 procent kvinnor och 39 procent män).

De direkta anslagen till universitet och högskolor motsvarar 4,1 procent av de samlade anslagen för statsbudgetens alla utgiftsområden. Universitetens och högskolornas samlade intäkter till forskning och utbildning på forskarnivå var 49,5 miljarder kronor 2022. Drygt 70 procent av forskningsmedlen kom från svenska staten, antingen som direkta statsanslag eller via olika myndigheter. De direkta statsanslagen var 21,6 miljarder för forskning och utbildning på forskarnivå.

52 Vissa handlingar i myndighetens forskningsverksamhet ska inte gallras, se 6–7 §§ Riksarkivets föreskrifter och allmänna råd om gallring av handlingar i statliga myndigheters forskningsverksamhet (RA-FS 1999:1). Exempel på forskningsdata som inte ska gallras kan vara särskilt omfattande och unikt primärmaterial, register och databaser med särskilt hög täckningsgrad eller data som rönt stor uppmärksamhet i den allmänna debatten, se bilaga 1B RA-FS 1999:01.

53 Uppgifterna i detta avsnitt avser 2022 och har hämtats från Universitetskanslersämbetet, *Universitet och högskolor. Årsrapport 2023,* 2023 samt prop. 2023/24:1, utg.omr. 16, s. 109.

54 Enskilda utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina.

Statliga universitet och högskolor styrs i första hand av högskolelagen (1992:1434) och högskoleförordningen (1993:100). Regeringen styr också statliga universitet och högskolor via årliga regleringsbrev. Statliga universitet och högskolor styrs även av de generella regelverk som gäller för andra statliga myndigheter.[55] Lärosätenas återrapportering av utfallet av sin verksamhet sker i första hand i årsredovisningarna. Lärosätena bestämmer själva över den interna fördelningen av resurser, utbildningsutbud, utbildningens innehåll och utformning, inklusive hur många studenter som antas och vilken forskning som lärosätet ska bedriva.[56]

Forskningens frihet är skyddad i regeringsformen (RF) och vidare reglerad i högskolelagen (1992:1434). Det innebär att forskningsproblem fritt får väljas, forskningsmetoder fritt får utvecklas och forskningsresultat fritt får publiceras.[57] 2021 skrevs även akademisk frihet in i högskolelagen. Här framgår att som allmän princip i högskolornas verksamhet ska gälla att den akademiska friheten ska främjas och värnas.[58] Forskning, i betydelsen fritt kunskapssökande och fri kunskapsspridning, ska dock alltid utövas inom de rättsliga ramar som finns.[59]

2.4 Lärosätenas interna styrning och organisation

Som en följd bland annat av den så kallade autonomireformen 2011 kan organisationen se olika ut på lärosätena.[60] I figur 2 nedan framgår ett typexempel på hur organisationen kan se ut och vilka akademiska och administrativa chefsnivåer som finns.

55 Det är dock inte alla bestämmelser i myndighetsförordningen (2007:515) som gäller för de statliga lärosätena. I 1 kap. 5 § högskoleförordningen anges vilka bestämmelser i myndighetsförordningen som inte tillämpas på de statliga lärosätena.

56 Universitetskanslersämbetet, ”Så styrs högskolesektorn”, hämtad 2023-09-05. Bestämmelser för Sveriges lantbruksuniversitet och Försvarshögskolan finns i förordningen (1993:221) för Sveriges lantbruksuniversitet respektive förordningen (2007:1164) för Försvarshögskolan.

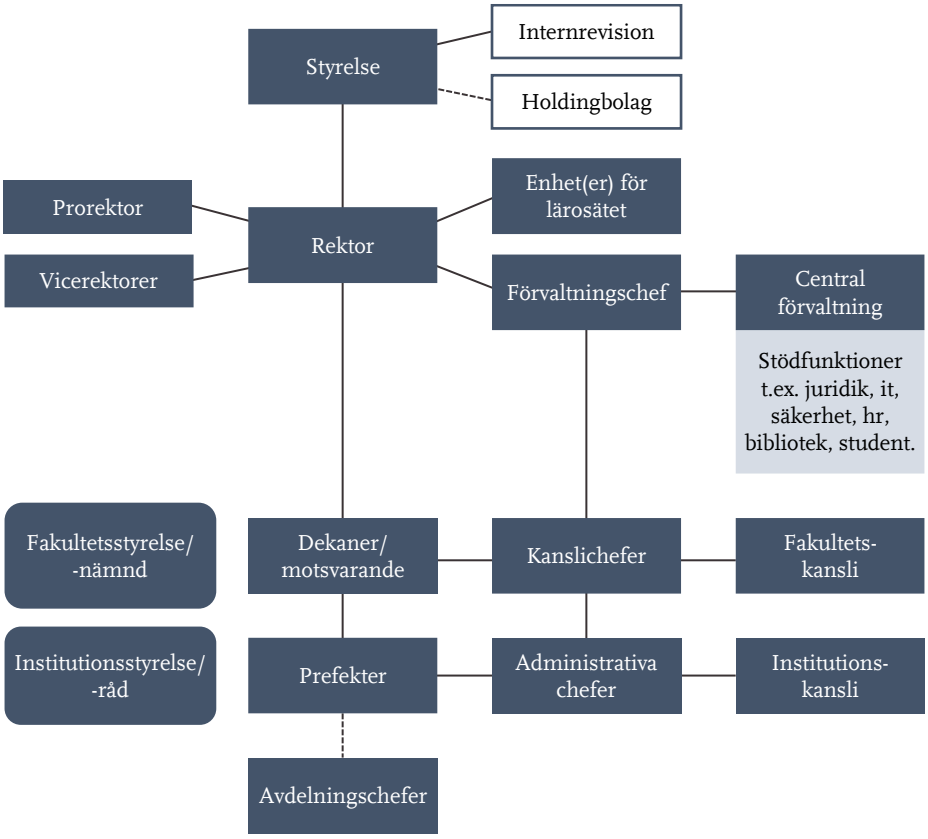
57 2 kap. 18 § regeringsformen; 1 kap. 6 § högskolelagen (1992:1434).

58 1 kap. 6 § högskolelagen (1992:1434).

59 Prop. 2020/21:60, s. 131, 192, bet. 2020/21:UbU16, rskr. 2020/21:254.

60 Prop. 2009/10:149. I SOU 2015:92 beskrivs t.ex. Lunds universitet som det mest decentraliserade av alla lärosäten, och att de fyra stora flerfakultetsuniversiteten Uppsala universitet, Lunds universitet, Göteborgs universitet och Stockholms universitet har mycket gemensamt ifråga om organisationsstruktur, delegering av beslutanderätt, tradition och kultur jämfört med övriga universitet och högskolor.

Figur 2 Typexempel på organisation vid ett lärosäte



Källa: Något omarbetad från figur 1.2 Norén och Wallin, Akademisk chef – hur fungerar det?, 2022, s. 30.

I den akademiska organisationen finns en eller flera fakulteter med ett antal institutioner under varje fakultet. Den akademiska chefslinjen går ofta från rektor till dekan till prefekt. Stora institutioner kan också ha avdelningar med avdelningschefer.[61] Kungl. Tekniska högskolan (KTH) och Lunds universitet (LU) är organisationer med tre akademiska organisatoriska nivåer.[62] Det finns också lärosäten som inte har en fakultetsnivå med dekaner. Vid dessa svarar prefekterna direkt mot rektor. Blekinge tekniska högskola (BTH) är ett exempel på ett lärosäte med fakulteter men där den akademiska chefslinjen går från rektor direkt till prefekt. Se vidare bilaga 3 för organisationsskisser för BTH, KTH och LU.

61 Norén och Wallin, *Akademisk chef – hur fungerar d*et?, 2022, s. 30–32.

62 LU har 9 fakulteter och 63 institutioner. KTH har 5 skolor och sammanlagt 27 institutioner. Därtill finns ett antal centrumbildningar.

I den administrativa förvaltningsorganisationen finns flera avdelningar, ibland med särskilda enheter eller funktioner under varje avdelning. Rektor är chef över förvaltningschefen i den administrativa chefslinjen. Förvaltningschefen är chef över förvaltnings- och stödverksamhetens avdelningschefer, och ibland även över chefer för förvaltning och stöd på fakultets- eller institutionsnivå.[63]

Roller och funktioner på lärosäten av relevans för informationssäkerhetsarbetet

En högskola beslutar om sin interna organisation utöver styrelse och rektor, om inte något annat är föreskrivet.[64] Det innebär att det finns en del variation i vilka som arbetar med informationssäkerhet på lärosätena, och hur arbetet organiseras, utformas och genomförs. Huvudansvaret för själva informationssäkerheten följer som regel verksamhetsansvaret. Nedan följer en typbeskrivning av huvudsakliga roller som vi bedömer är relevanta för informationssäkerhetsarbetet.[65]

Styrelsen: styrelsen har inseende över lärosätets alla angelägenheter och svarar för att dess uppgifter fullgörs. Styrelsen beslutar bland annat i viktigare frågor om lärosätets övergripande inriktning, dess organisation, interna resursfördelning och uppföljning. I övriga uppgifter och frågor ska rektor besluta, om inte något annat angetts av lag eller förordning eller beslutats av styrelse. Vid statliga universitet och högskolor utser regeringen ordföranden och ytterligare sju ledamöter i styrelsen. Lärare och studenter vid högskolan har rätt att utse tre ledamöter vardera i styrelsen. Rektor ingår i styrelsen.[66]

Rektor: ansvarig för ledningen av verksamheten närmast under styrelsen. Vid statliga universitet och högskolor anställs rektor av regeringen efter förslag från lärosätets styrelse. Rektor anställs för högst sex år, anställningen får förnyas, dock högst två gånger om vardera högst tre år.[67] Rektor ansvarar för att verkställa beslut och fastställa delegationer för beslutsbefogenheter.

Prorektor: utses av lärosätesstyrelsen och är ställföreträdande för rektor. Prorektorn har därutöver egna ansvarsområden.

Vicerektor: en eller flera, ansvariga för vissa verksamhetsområden som exempelvis forskning, internationalisering eller digitalisering. Utses av rektor.

63 Norén och Wallin, *Akademisk chef – hur fungerar d*et?, 2022, s. 31.

64 2 kap. 5 § högskolelagen (1992:1434).

65 Utöver de referenser som anges i fotnoter är informationen i första hand hämtad från SOU 2015:92; Norén och Wallin, *Akademisk chef – hur fungerar det?,* 2022, s. 180–181 och bilaga 2 samt baserad på information som Riksrevisionen inhämtat under granskningen.

66 2 kap. 2–4 §§ högskolelagen (1992:1434); 2 kap. 1–3, 7–7 b §§ högskoleförordningen (1993:100). Regeringen meddelar särskilda föreskrifter om sammansättningen av styrelse vid Sveriges lantbruksuniversitet och vid Försvarshögskolan samt om en nämnd för forskning och utbildning vid Försvarshögskolan, se 2 kap. 9 § högskolelagen (1992:1434).

67 2 kap. 3 § högskolelagen (1992:1434); 2 kap. 8 § högskoleförordningen (1993:100).

Dekan: högsta akademiska chef på en fakultet/ordförande i en fakultetsnämnd. Vanligen rekryterad ur lärarkåren på ett tidsbegränsat uppdrag. Utses av rektor. Har ofta övergripande verksamhets-, budget- och personalansvar för fakulteten.

Prefekt: högsta akademiska chef på en institution eller motsvarande. Vid stora institutioner kan det finnas avdelningschefer mellan prefekt och forskare. Prefekten är ofta själv lärare/forskare och uppdraget är oftast ett deltidsuppdrag. Det varierar hur prefekter utses – de kan vara valda eller föreslagna av sina egna kollegor och utses av dekan eller annan överordnad chef såsom rektor. Prefektens mandatperiod är oftast tidsbegränsad (vanligtvis tre eller fyra år) men kan förlängas. Prefekten är en länk mellan forskande och undervisande personal och fakultets- och lärosätesledningarna, med ansvar bland annat för att beslut implementeras på institutionen. Prefekten skriver även på avtal om mottagande av forskningsbidrag upp till vissa belopp.

Lärare och forskare: den forskande och undervisande personal som i huvudsak bedriver forskning och undervisning i högskolan består av professorer, lektorer, meriteringsanställda (forskarassistenter, biträdande lektorer och postdoktorer), adjunkter och annan forskande och undervisande personal med eller utan doktorsexamen (t.ex. forskare, forskningsingenjörer och forskningsassistenter).[68]

Doktorand: genomgår utbildning på forskarnivå och innehar i de flesta fall en doktorandanställning. Inom naturvetenskap och teknik är 6 procent respektive 12 procent företagsdoktorander vilket betyder att de bedriver sin forskarutbildning inom ramen för en anställning utanför högskolan.[69]

Förvaltningschef och verksamhetsstöd: förvaltningschefen är högsta chef för förvaltnings- och stödverksamheten. Anställs av rektor, som är närmaste chef. Andra benämningar är universitetsdirektör eller högskoledirektör. Inom förvaltnings- och stödverksamheten finns ofta flera funktioner med roller i lärosätets informationssäkerhetsarbete, såsom säkerhetschef, it- och it-säkerhetsansvariga, jurister, exportkontrollhandläggare och dataskyddsombud.

Informationssäkerhetschef/Chief Information Security Officer (CISO): leder och samordnar det strategiska informationssäkerhetsarbetet vid lärosätet. Exempel på mandat som CISO kan ha är att kravställa utvecklingsprojekt, bedriva tillsyn att styrdokument efterlevs och att rapportera interna brister i efterlevnaden av styrdokument.[70] Har ibland personalansvar om det även finns t.ex. *informationssäkerhetsspecialister* eller *informationssäkerhetsstrateger* anställda på lärosätet.

---

68 Universitetskanslersämbetet, *Universitet och högskolor, Årsrapport 2023*, s. 94–95.
69 Universitetskanslersämbetet, *Universitet och högskolor, Årsrapport 2023*, s. 82–83.
70 MSB:s metodstöd för systematiskt informationssäkerhetsarbete, informationssäkerhet.se, ”Metodstöd, Utforma, CISO-rollen, Mandat som CISO”, hämtad 2023-10-30.

It: it-avdelningen leds vanligtvis av en it-chef med övergripande ansvar för lärosätets it-organisation inom verksamhetsstödet. Där finns ofta medarbetare med ansvar för användarstöd, infrastruktur, säkerhet, arkitektur, tjänsteutbud, drift, systemförvaltning och systemutveckling inom it. På vissa lärosäten finns det även it-organisationer på fakultets- eller institutionsnivå.

Bibliotek och forskningsdatastöd: vid lärosätenas bibliotek finns medarbetare som jobbar med stöd kring forskningsdata, såsom tillgängliggörande, bevarande och hantering i enlighet med gällande regelverk. Ofta finns forskningsdatateam (som kan kallas *Data Access Unit*, DAU). Medabetare inom forskningsdatastöd hjälper ofta till i samband med forskningsansökningar och mottagande av extern finansiering, såsom upprättandet av datahanteringsplaner. Bibliotek och forskningsdatastöd kan också finnas på fakultetsnivå.

2.5 Regeringens styrning av lärosätena med koppling till säkerhet och informationssäkerhet

Regeringen har i första hand styrt lärosätenas informationssäkerhetsarbete genom generella förordningar och indirekt genom uppdrag till MSB.[71]

Från och med 2019 har olika aspekter av säkerhet varit med på dagordningen för de årliga myndighetsdialogerna med lärosätena. 2019 och 2020 togs säkerhetsskydd upp. 2021 och 2022 breddades punkten till säkerhetsfrågor, som inkluderar såväl informationssäkerhet som mer it-nära frågor, it-incidenter samt exportkontroll och säkerhetsskydd.[72]

2020 uppmanade den dåvarande ministern för högre utbildning och forskning lärosätesledningarna att bedriva ett systematiskt säkerhetsarbete i syfte att skapa sig en förståelse av eventuella skyddsvärden. Bakgrunden var bland annat den då relativt nya säkerhetsskyddslagen (2018:585).[73]

I det gemensamma regleringsbrevet avseende universitet och högskolor för 2022 var kravet att i årsredovisningen övergripande redovisa hur man arbetar för att stärka sin informationssäkerhet. I regleringsbrevet för 2023 låg fokus bland annat på att rapportera om den interna styrningen och uppföljningen av

71 Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och förordningen (2022:524) om statliga myndigheters beredskap.

72 Se Regeringskansliet, Utbildningsdepartementet, Dagordningar för myndighetsdialoger med Blekinge tekniska högskola, KTH och Lunds universitet 2019–2022.

73 Regeringskansliet, Utbildningsdepartementet, Ministern för högre utbildning och forskning, *Vikten av ett systematiskt säkerhetsarbete*, U2020/03059/UH, 2020-05-06.

informationssäkerhetsarbetet, it-incidenter samt hot- och sårbarhetsanalyser om rådande omvärldsläge. Rapportering skedde separat i oktober 2023.[74]

I juli 2023 fick Universitets- och högskolerådet, Vetenskapsrådet och Verket för innovationssystem (Vinnova) i uppdrag att ta fram vägledande nationella riktlinjer för internationella samarbeten. Riktlinjerna syftar till att stötta lärosätena att göra bedömningar av pågående och potentiella internationella utbildnings- och forskningssamarbeten. Uppdraget ska slutredovisas i december 2024.[75]

I augusti 2023 fick en utredare i uppdrag att biträda Utbildningsdepartementet med att se över hur det kan säkerställas att det finns kompetens om säkerhetsfrågor bland de ledamöter som utses av regeringen i de statliga universitetens och högskolornas styrelser. I uppdraget, som ska slutredovisas 31 december 2023, ingår även att bedöma om det finns behov av ytterligare åtgärder för att öka universitetens och högskolornas kompetens i säkerhetsfrågor, och i så fall föreslå sådana åtgärder.[76] Uppdraget föregicks av att lärosätesstyrelsernas mandatperioder kortades ned från 36 till 17 månader med motiveringen att det säkerhetspolitiska läget gör det nödvändigt att sådan kompetens ingår i styrelserna.[77]

2.6 Internationalisering och målet om ett öppet vetenskapssamhälle

Till skillnad från annan typ av information som hanteras på ett lärosäte, till exempel personalstatistik eller statistik om studenter, behöver forskningsdata ofta vara tillgängliga för en bredare krets aktörer. Det kan handla om att dela data inom en forskargrupp med såväl nationella som internationella samarbetspartner, med externa samarbetspartner, företag eller med tidskrifter i samband med publicering. Att arbeta med informationssäkerhet i en sådan kontext skapar särskilda utmaningar.

I den senaste forskningspropositionen skriver regeringen att det krävs en hög grad av internationalisering för att Sverige ska kunna vara en ledande forsknings- och kunskapsnation.[78] Av högskolelagen framgår att den samlade internationella verksamheten vid varje högskola ska stärka kvaliteten i högskolans utbildning och

74 Regeringsbeslut U2021/04851 (delvis), U2021/04891; regeringsbeslut U2022/02763, U2022/02805, U2022/02810 m.fl.

75 Regeringsbeslut U2023/02127.

76 Regeringskansliet, Utbildningsdepartementet, *Uppdrag att ta fram förslag om hur universitets och högskolors kompetens i säkerhetsfrågor kan öka*, U2023/02485, 2023-08-31.

77 Utbildningsdepartementet, ”Pressmeddelande: Nya styrelser för 30 universitet och högskolor”, 2023-04-27.

78 Prop. 2020/21:60, bet. 2020/21:UbU16, s. 27, rskr. 2020/21:254.

forskning.[79] Även inom sektorn ses internationalisering i allmänhet som ett medel för att öka kvaliteten i såväl forskning som utbildning.[80]

Regeringen anger att öppenhet bör utgöra grunden i internationellt samarbete, samtidigt som det behöver finnas en medvetenhet om behovet av att skydda nationella säkerhetsintressen, kunskap och teknik.[81] I samarbete med Kina nämns exempelvis utmaningar i fråga om etik, akademisk frihet och immaterialrättsskydd, samt kopplingar till den militära sektorn.[82]

Parallellt med ökad internationalisering pågår sedan en längre tid en omställning mot ett öppet vetenskapskapssamhälle som ska vara genomförd 2026. Det inkluderar såväl vetenskapliga publikationer som konstnärliga verk och forskningsdata. Av forskningspropositionen 2016/17:50 framgår att begränsningar kan motiveras av integritetsskäl, nationella säkerhetsintressen eller immaterialrättsliga skäl, men att öppen tillgång utgör normen och inskränkningar i öppenheten utgör undantagen.[83] I proposition 2022/23:1 understryker regeringen att det finns ett fortsatt stort behov av att nyckelaktörer som lärosäten och forskningsfinansiärer tar ett gemensamt ansvar för att verka för att den nationella riktningen för öppen tillgång följs och uppnås. [84]

Lärosätenas uppdrag att utveckla arbetet med öppen vetenskap anges i regleringsbrev.[85] Vad gäller forskningsdata ska omställningen vara genomförd fullt ut senast 2026, vilket innebär att forskningsdata ska göras tillgängliga så öppet som möjligt och så begränsat som nödvändigt.[86] Vetenskapsrådet har uppdraget att samordna, följa upp och främja samverkan i arbetet för öppen tillgång till forskningsdata.[87] Vetenskapsrådet rekommenderar att forskningsdata (och metadata) som finansieras av offentliga medel och som kan publiceras med öppen tillgång hanteras i enlighet med de så kallade FAIR-principerna. Det innebär att forskningsdata hanteras på ett sätt som gör att de blir sökbara (findable),

79 1 kap. 5 § högskolelagen (1992:1434).

80 Se t.ex. SOU 2018:3, s. 71–72.

81 Regeringsbeslut U2023/02127; Regeringskansliet, Näringsdepartementet, *Nationell inriktning för artificiell intelligens N2018.14*, s. 9.

82 Dir. 2019:50; dir. 2020:52; skr. 2017/18:259; skr. 2019/20:18, s. 18.

83 Prop. 2016/17:50. Se också prop. 2012/12:30, s. 150, där regeringen anger att Vetenskapsrådet bör få i uppdrag att utveckla former och nationella riktlinjer för hur forskare kan få öppen tillgång till forskningsresultat och forskningsdata.

84 Prop. 2022/23:1, utg.omr. 16, s. 218.

85 Regeringsbeslut U2022/02763, U2022/02805, U2022/02810 m.fl.

86 Prop. 2020/21:60, s. 101.

87 2 § 21 förordning (2009:975) med instruktion för Vetenskapsrådet.

tillgängliga (accessible), interoperabla (interoperable), och återanvändningsbara (reusable).[88]

Regeringen anger datahanteringsplaner som en första insats för att främja god datahantering.[89] Redan 2012 ställde Vetenskapsrådet krav på datapubliceringsplaner för att bevilja ansökningar med stora faktainsamlingar i syfte att säkerställa framtida återanvändning av forskningsdata.[90] Sedan 2019 finns krav på att forskare som beviljas anslag ska upprätta en datahanteringsplan. Planen ska beskriva hur insamlade data ska hanteras under och efter forskningsprocessen och inkluderar att redogöra för hur det säkerställs att data hanteras enligt de rättsregler som gäller till exempel hantering av personuppgifter, sekretess och immaterialrätt.[91]

Sedan 2022 inkluderar lagen (2022:818) om den offentliga sektorns tillgängliggörande av data även forskningsdata.[92] Syftet är att främja den offentliga sektorns tillgängliggörande av data för vidareutnyttjande, särskilt i form av öppna data. Statliga universitet och högskolor ska tillämpa lagen bara i fråga om forskningsdata. Tillgängliggörande gäller under förutsättning att krav på informationssäkerhet och skydd av personuppgifter kan upprätthållas och att det inte innebär risker för Sveriges säkerhet.[93]

88 Vetenskapsrådet, ”Tillgängliggörande av forskningsdata och FAIR-kriterier”, hämtad 2023-09-05.
89 Prop. 2020/21:60, s. 101, bet. 2020/21:UbU16, rskr. 2020/21:254.
90 Mannberg-Zackari, ”Fler citeringar med återbruk av data”, 2012-08-20.
91 Vetenskapsrådet, *Vägledning till mallen för datahanteringsplaner*, 2022, s. 8.
92 Lagen föregicks av lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen som inte inkluderade forskningsdata utan endast handlingar som finns hos högskolebibliotek (3 § ibid.).
93 1 och 6 §§ lagen (2022:818) om den offentliga sektorns tillgängliggörande av data.

3 Lärosätenas arbete med att identifiera skyddsvärda forskningsdata och att analysera informationssäkerhetsrisker

I det här kapitlet besvarar vi frågan om universitet och högskolor arbetar effektivt med att identifiera skyddsvärda forskningsdata och att analysera informationssäkerhetsrisker. Våra huvudsakliga iakttagelser sammanfattas nedan.

3.1 Riksrevisionens huvudsakliga iakttagelser

- Det sker ingen systematisk klassning av forskningsdata enligt lärosätenas framtagna modeller för informationsklassning. Det kan leda till att vissa skyddsvärda forskningsdata inte identifieras. Istället värderas vissa forskningsdata mer eller mindre formaliserat av forskare på grund av externa krav, exempelvis i datahanteringsplaner. Det är dock inte alla forskningsprojekt som har datahanteringsplaner. När lärosätena saknar en överblick över skyddsvärda forskningsdata kan det leda till bristande skydd.
- Det finns flera exempel på institutioner och enskilda forskargrupper som har egna it-lösningar utanför den centrala it-infrastruktur som lärosätet tillhandahåller, bland annat när det gäller lagring och säkerhetskopiering av data. Därmed försvåras lärosätenas möjligheter att identifiera gemensamma behov av it-lösningar vilket kan leda till varierande och bristande informationssäkerhet.
- Eftersom klassningen av forskningsdata inte görs systematiskt saknas det underlag för riskbedömningar på institutioner och central lärosätesnivå. Riskbedömningarna inkluderar sällan informationssäkerhet kring forskningsdata. Dessutom rapporterar lärosätena få it-incidenter. Det kan leda till att lärosätena inte åtgärdar säkerhetsbrister och därmed inte heller inför ändamålsenliga säkerhetsåtgärder.

3.2 Lärosätena arbetar inte systematiskt för att inventera och klassa forskningsdata

Granskningen visar att få forskare klassar sina forskningsdata i enlighet med lärosätenas modeller för informationsklassning. Många forskare gör istället mindre formaliserade bedömningar av sina forskningsdata. De dokumenteras inte alltid, eller dokumenteras i enlighet med krav från externa samarbetspartner eller

forskningsfinansiärer. Det finns ingen samlad dokumentation över dessa mindre formaliserade bedömningar. När lärosätena saknar en överblick över skyddsvärda forskningsdata kan det leda till att dessa inte skyddas på ett ändamålsenligt sätt. Eftersom det saknas systematik i inventering, klassning och riskanalys är det svårt för lärosätena att dimensionera och anpassa säkerhetsåtgärder och it-tjänster efter de behov som finns i forskningsverksamheten. Det kan i slutändan leda till att obehöriga får tillgång till skyddsvärda forskningsdata. Företrädare för Säkerhetspolisen uppger att externa aktörer otillbörligen har skaffat sig åtkomst till känslig forskning vid svenska lärosäten.[94]

3.2.1 Få lärosäten har inventerat forskningsdata

15 av 24 lärosäten uppger att de har inventerat sin information, men endast ca hälften av de 15 lärosätena uppger att inventeringen har inkluderat forskningsdata. I de flesta fall har forskningsdata endast inventerats till viss del. Det resulterar i att lärosätena inte får en helhetsbild över de forskningsdata som finns på lärosätet. Flera lärosäten anger att de på sikt ska inventera processerna för forskning.[95]

Vid Blekinge tekniska högskola (BTH), Kungl. Tekniska högskolan (KTH) och Lunds universitet (LU) sker inte inventering av information med utgångspunkt i ett systematiskt informationssäkerhetsarbete i forskningsverksamheterna. Vid KTH sker olika typer av kartläggning exempelvis genom arkivfunktionen, informationshanteringsplaner och diverse initiativ till kartläggning från informationssäkerhetschef/motsvarande.[96] Det förekommer även ärendehanteringssystem och databaser för forskningsavtal som ger viss möjlighet till kartläggning.[97] Olika funktioner vid KTH och LU försöker också inventera forskningsdata genom exempelvis enkäter, nulägesanalyser och riskanalyser.[98] Arbetet är i regel inte samordnat och sker inte med systematik. Det är heller inte heltäckande i meningen att alla forskningsdata inkluderas.

3.2.2 Forskningsdata klassas inte enligt en gemensam modell

Av intervjuer med forskare vid BTH, KTH och LU framgår att det är ovanligt att forskare klassar sina data systematiskt och enligt lärosätets beslutade modell, trots

94 Intervju med företrädare för Säkerhetspolisen, 2023-03-24.
95 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.
96 Intervju KTH7.
97 T.ex. CASE på KTH, intervju KTH4.
98 Intervjuer KTH12; LU7.

att det finns en målbild att det ska göras.[99] Brister avseende både modeller för informationsklassning och genomförande av informationsklassning har även tagits upp i internrevisionsrapporter vid LU och KTH.[100] Riksrevisionen har också tagit del av resultat från MSB:s självskattningsverktyg Infosäkkollen 2021, som visar på genomgående brister i lärosätenas arbete med informationsklassning.[101]

I Riksrevisionens enkät uppger 21 av 24 lärosäten att de har en modell för informationsklassning. Det är vanligast att modellerna ska tillämpas på it-system och it-tjänster samt informationsmängder[102] (17 lärosäten vardera). Nästan lika många lärosäten uppger att modellen ska tillämpas på informationstyper[103]. Forskningsdata kan bestå av olika informationstyper, exempelvis personuppgifter. I den meningen finns det därmed delar av forskningsdata som informationsklassas enligt lärosätenas framtagna modeller. Ett lärosäte beskriver i vår enkät att informationsklassning av forskningsprojekt sker inför start av nya forskningsprojekt. Klassningen görs med hjälp av bland annat it-säkerhetsansvariga och jurister med GDPR-kompetens. Lärosätet beskriver vidare att detta arbetssätt har gjort det möjligt att utforma ett register över alla skyddsvärda informationsbehandlingar som görs i forskningsprojekt.[104]

Bristande systematik för klassning av forskningsdata gör det överlag svårt att sammanställa vilka data som faktiskt är skyddsvärda. 8 av 24 lärosäten uppger i enkäten att de har en samlad förteckning över verksamhetens skyddsvärda informationstillgångar. Av dessa 8 är det dock bara 5 lärosäten som inkluderat vissa eller alla skyddsvärda forskningsdata. Av de som inte har upprättat en förteckning

---

99 Intervjuer BTH3; BTH9; BTH10; KTH2; KTH4; LU7; LU15; LU25; Blekinge tekniska högskola, *Riktlinjer för informationssäkerhet vid Blekinge Tekniska Högskola,* version 1.0, 2012-06-19; KTH, Anvisning *Informationsklassificering för KTH*, gäller från och med 2015-01-01; Lunds universitet, *Riktlinjer för informationssäkerhet vid Lunds universitet,* 2017-06-22. Den beslutade modellen vid LU implementerades aldrig och var i vissa delar föråldrad i förhållande till MSB:s föreskriftskrav. Det pågår därför ett arbete med att ersätta modellen uppger CISO vid Lunds universitet i mejlsvar, 2023-09-13.

100 Lunds universitet, Internrevisionen, *Granskning av cyber- och informationssäkerhet,* 2019-12-13; Lunds universitet, Internrevisionen, *Granskning av fysisk säkerhet i IT-utrymmen*, 2022-12-20; KTH, *Granskning av KTH:s ledningssystem för informationssäkerhet, Revisionsrapport 1/2020,* 2020-10-01.

101 15 lärosäten inkom med svar på Infosäkkollen 2021.

102 Se ordlista.

103 Se ordlista.

104 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1. En stor del av lärosätena uppger att de arbetar med att ta fram interna rutinbeskrivningar och metodstöd eller reviderar informationsklassningsmodeller. En tredjedel av lärosätena uppger att informationsklassning prioriterats de senaste två åren. Bara 1 av 24 lärosäten lyfter informationsklassning som något som fungerar bra vid en öppen fråga om vad i lärosätets informationssäkerhetsarbete som fungerar bra.

anger ett lärosäte att man bedömer att informationen inte är av den klass att det behövs en förteckning. Andra lärosäten beskriver att de endast har det för en viss typ av skyddsvärda data, som exempelvis säkerhetsskyddsklassificerade uppgifter eller personuppgifter.[105]

3.2.3 Skyddsvärda forskningsdata fångas sällan upp systematiskt på institutionerna

Granskningen visar att prefekter har otillräcklig kunskap om huruvida skyddsvärda forskningsdata hanteras vid institutionen. Det saknas ofta formaliserade arbetssätt för att identifiera, dokumentera och förmedla skyddsvärden och skyddsbehov till central lärosätesnivå. Enligt Riksrevisionen är det viktigt att skyddsvärden identifieras i forskningsverksamheten, eftersom forskarna själva känner sina data bäst. Riksrevisionen konstaterar att det är svårt för de flesta prefekter att ha tillräcklig kännedom om alla skyddsvärda data på en stor institution. Men prefekten kan följa upp att forskningsledarna regelbundet inventerar och klassar sina forskningsdata.

Prefekterna i vår granskning har olika syn på möjligheterna att ha kännedom om de skyddsvärda forskningsdata som hanteras på deras respektive institutioner. Vissa prefekter framhåller att det är forskarna själva som är ansvariga för att bedöma om deras forskningsdata är skyddsvärda och vidta nödvändiga åtgärder. Det finns också en uppfattning att det ingår i prefektens ansvar att tänka igenom vad som kan vara skyddsvärt innan ett projekt startar. Vidare beskriver vissa prefekter att de har kännedom genom signering av finansieringsplaner och genom att hålla sig uppdaterade om alla nya forskningsprojekt som startar vid institutionen.[106]

Flera prefekter menar att de vet vilka skyddsvärda forskningsdata som hanteras av forskarna vid institutionen genom att det i externa samarbeten skrivs avtal där datahantering är reglerat eller hänvisar till att skyddsvärda forskningsdata säkerhetsklassificeras av företaget forskarna samarbetar med. En del prefekter säger däremot att de omöjligen kan ha överblick över alla skyddsvärda forskningsdata vid sina institutioner, bland annat på grund av den stora mängd data som hanteras. Vid ett tillfälle hade en prefekt precis innan vår intervju tillfrågat alla forskningsledare på institutionen om de hanterade skyddsvärda data och samlat in informationen.[107] Det visar att det med en rimlig arbetsinsats går att få en överblick över om skyddsvärda forskningsdata hanteras vid institutionen.

---

105 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 2.
106 Intervjuer BTH6; BTH8; KTH11; KTH9; KTH10; KTH13; LU17.
107 Intervjuer BTH5; BTH6; BTH8; KTH13; KTH15; LU16; LU17.

I intervjuer anges flera orsaker till att kännedomen om skyddsvärda forskningsdata varierar mellan institutioner. Det kan exempelvis bero på olika grad av mognad avseende informationssäkerhet inom vissa forskningsområden, vilket i sin tur kan bero på att vissa områden har externa standarder och nationella eller internationella regelverk som reglerar bland annat datahantering. Andra orsaker som uppges i intervjuerna är varierande intern informationssäkerhetskultur och institutionens storlek och forskningsbredd.[108]

3.2.4 Forskare gör mindre formaliserade bedömningar av forskningsdatas skyddsvärde som inte dokumenteras

Eftersom många forskare gör mindre formaliserade bedömningar av sina forskningsdata som inte dokumenteras saknas underlag för samlade riskbedömningar på institutions- och lärosätesnivå. Vi har observerat fall där enskilda forskare med kompetens och vilja gör informationsklassningar enligt gemensam lärosätesmodell, men det är ovanligt. I flera intervjuer uppger forskare att de använder sunt förnuft för att bedöma känsligheten i sina forskningsdata. Det finns också en ”man bara vet”-mentalitet gällande om huruvida man hanterar skyddsvärda data eller inte. En annan uppfattning är att det inte finns något externt intresse för ens forskningsdata.[109]

Flera forskare beskriver dessutom att det bara är under en kortare period som det finns behov av att skydda sina forskningsdata eftersom de ändå görs tillgängliga så fort man publicerar sina resultat. Det som däremot är unikt och skyddsvärt är specifika arbetsmetoder, till exempel hanteringen av material i ett laboratorium, som inte framgår av publicerade data.[110] Andra forskare menar att rådata i form av exempelvis mätningar är obegripliga för utomstående som inte har kontexten.[111] Riksrevisionen gör ingen bedömning av rimligheten i dessa påståenden, men konstaterar att en systematisk och dokumenterad informationsklassning av ens forskningsdata möjliggör att ändamålsenliga säkerhetsåtgärder lättare kan identifieras och införas. I ovan nämnda fall skulle det vara att hantera loggböcker eller material, som behövs för att tolka rådata eller annat material och resultat, som skyddsvärda.

---

108 Intervjuer BTH8; KTH2; KTH3; KTH6; KTH13.

109 Intervjuer BTH3; BTH11; BTH13; KTH6; KTH9; KTH10; KTH16; KTH18; KTH20; LU28; LU29.

110 Intervjuer KTH9; LU21. Innovationsrådgivare vid ett lärosäte beskriver att det ofta är ett verktyg eller metod som använts för att komma fram till resultat som forskare vill ta patent på, snarare än resultatet som sådant. Intervju med företrädare för innovationskontoret Fyrklövern, 2022-09-21.

111 Intervjuer KTH10; KTH13; LU21.

3.2.5 Externa samarbetspartner ställer krav på säker hantering av forskningsdata

Externa samarbetspartner och finansiärer ställer olika krav på att forskningsdata ska hanteras i enlighet med skyddsvärdet. Det dokumenteras ofta i en datahanteringsplan eller i särskilda sekretessavtal. Granskningen visar att denna dokumentation inte finns samlad vid lärosätena. Därmed saknas underlag för samlade riskbedömningar på institutions- och lärosätesnivå.

Vidare visar granskningen att det råder en uppfattning om att de krav som externa samarbetspartner och finansiärer ställer på säker datahantering ofta är tydligare än lärosätenas egna krav. I granskningen framkommer också att såväl forskare som externa partner menar att en säker hantering av skyddsvärda data blir ”självreglerande” eftersom forskare som inte sköter sig riskerar att ses som säkerhetsbelastningar och därmed olämpliga forskningspartner.[112]

Den externa samarbetspartnern ansvarar för att informationsklassa sina egna forskningsdata och anpassa hanteringen efter dem. Som forskare behöver man vara medveten om vilket ansvar man har när data förs över och hanteras vid lärosätet. Det kan vara en särskild utmaning att bedöma sådana forskningsdata i kombination med andra data som finns på lärosätet. Vi har dock iakttagit att skyddsvärda forskningsdata ofta behandlas på den externa partnerns utrustning och/eller i dens lokaler. Det förekommer också att till exempel doktorander genomgår säkerhetsprövning och har sin arbetsplats hos den externa partnern. Forskare nämner även samarbeten med exempelvis Försvarets materielverk och Svenska kraftnät som kräver säkerhetsprövning för deltagande.[113] Vidare beskriver forskare vid BTH ett samarbete med Trafikverket där tillgången till data är väldigt begränsad. Liknande hantering beskrivs av verksamma vid KTH och LU. Exempelvis finns forskare vid KTH som samarbetar med Karolinska institutet (KI) där forskningsdata ligger på KI och forskare vid LU som använder data från Region Skåne.[114]

---

112 Intervjuer BTH8; BTH11; BTH13; BTH14; KTH4; KTH9; KTH14; KTH17; LU17; intervju med företrädare för SSAB, 2022-11-02; intervju med företrädare för Jernkontoret, 2022-11-05; intervju med företrädare för RISE Research Institutes of Sweden, 2022-11-25.

113 Intervjuer BTH3; BTH13; KTH2; KTH4; KTH6; KTH9; KTH13; KTH20. En befattning placeras i säkerhetsklass utifrån tillgång till säkerhetsskyddsklassificerade uppgifter eller den skada den kan åsamka den säkerhetskänsliga verksamheten. En anställning i staten, en kommun eller en region som är placerad i säkerhetsklass 1 eller 2 får endast innehas av den som är svensk medborgare, se 3 kap. 5–9, 11 §§ säkerhetsskyddslagen (2018:585). Säkerhetsprövning kan också genomföras utan inplacering i säkerhetsklass, se mejl från företrädare för Länsstyrelsen Stockholm med synpunkter på rapportutkast från Riksrevisionen, 2023-10-25.

114 Intervjuer BTH8; BTH13; KTH10; KTH18; KTH17; LU27.

Vilken information som är konfidentiell kan regleras i ett sekretessavtal (så kallat non-disclosure agreement, NDA) mellan forskare och extern partner inför ett samarbete. Detta gäller framför allt affärshemligheter, men kan även gälla forskningssamarbeten om militär utrustning eller kritisk infrastruktur.[115]

Enligt KTH:s delegationsordning ska alla forskningsavtal granskas av affärsjurister. Som forskare ska man bland annat ange om någon av partnerna i avtalet tillför så kallad bakgrundsinformation (exempelvis tidigare genererade resultat eller material) samt om konfidentiell information kommer att utbytas.[116] Vid skolorna tar man stort stöd av det juridiska stödets rådgivande funktion.[117] Vid BTH finns ingen jurist anställd utan vid behov anlitas juriststöd.[118] LU:s juridiska stöd är frivilligt och granskar ca 800 avtal om året från hela lärosätet.[119] Vid varken KTH eller LU har det rättsliga stödet kännedom om alla avtal. Det händer att man får in avtal som forskare själva förhandlat, obehörigt skrivit under och som inte granskats av lärosätets jurister.[120] Detta kan medföra både oönskade informations-säkerhetsrisker och ekonomiska risker för lärosätena.

3.2.6 Värdering av forskningsdata kan ske i datahanterings-planer, men alla forskare använder sig inte av dem

Flera finansiärer[121] ställer krav på datahanteringsplaner vid beviljade forskningsansökningar men det finns ingen systematik vid lärosätena rörande hur dessa hanteras. I datahaneringsplanerna ska forskare beskriva hur ens forskningsdata ska hanteras under och efter forskningsprocessen.[122] Hantering av skyddsvärda data är en del i planen.[123]

---

115 Intervjuer KTH4; KTH12; KTH14; KTH15.

116 KTH, ”Avtalshantering”, hämtad 2023-09-05.

117 Intervju KTH4.

118 Intervjuer BTH1; BTH2.

119 Intervju LU10.

120 Intervjuer KTH8; LU10. Den avtalsdatabas som sattes upp vid KTH 2019, CASE, har underlättat överblicken och att identifiera avtalen, eftersom alla avtal inte diarieförs i lärosätets ärendehanteringssystem, intervju KTH8.

121 Bl.a. Vetenskapsrådet (sedan 2019), Forskningsrådet för miljö, areella näringar och samhällsbyggnad (Formas) och EU:s forskningsprogram Horisont 2020 (från 2017).

122 Vetenskapsrådet, ”Datahanteringsplaner”, hämtad 2023-05-24.

123 I planen kan det finnas kontrollfrågor om immateriella rättigheter, känsliga personuppgifter och diverse etiska och juridiska frågeställningar. I Vetenskapsrådets mall finns två rubriker som rör säker hantering av data, nämligen *Lagring och säkerhetskopiering* samt *Rättsliga och etiska aspekter*. En vägledning utvecklar frågorna i mallen, se Vetenskapsrådet, 2022; Vetenskapsrådet, ”Mall för datahanteringsplaner”, hämtad 2023-04-25. I den mall som tillhandahålls av Svensk nationell datatjänst (SND) lyfts konfidentiell information som en aspekt, exemplifierat med persondata och säkerhetsklassade data. (Riksrevisionen noterar att säkerhetsklassad data bör avse *säkerhetsskyddsklassificerade* data.) SND har en mer utvecklad vägledning i form av en

Vetenskapsrådet kontrollerar inte att datahanteringsplanerna faktiskt lämnas in i samband med ansökan utan lägger ansvaret på medelsförvaltaren, det vill säga lärosätet.[124] I granskningen har vi inte iakttagit att det på de tre exempellärosätena förekommer någon systematisk uppföljning av om forskarna verkligen lämnar in sina planer, eller uppdaterar dem under forskningsprojektets gång. Riksrevisionen konstaterar att det inte heller görs någon sammanställning av upprättade datahanteringsplaner på något av de tre exempellärosätena. Det finns en ambition att datahanteringsplanerna ska diarieföras. Vid LU finns ett centralt diarieföringssystem på lärosätesnivå men det används inte till alla handlingar av alla fakulteter.[125] Det är också en utmaning att veta vilken version av datahanteringsplanen som ska diarieföras och arkiveras eftersom den löpande ska kunna uppdateras, så kallad versionering. Nuvarande ärendehanteringssystem vid KTH har exempelvis inte stöd för versionering, Vid både KTH och LU pågår arbete på central lärosätesnivå och vid fakulteter för att försöka få överblick över datahanteringsplaner i databaser eller liknande.[126]

Vid vissa universitet är hanteringen av datahanteringsplaner formaliserad via prefekten. Vid till exempel Uppsala universitet ska prefekten vid den anslagsförvaltande institutionen intyga att en datahanteringsplan är upprättad innan projektet godkänns i forskningsfinansiärernas ansökningssystem Prisma.[127] En utmaning som nämns i vår granskning är dock att man som prefekt inte har kompetens att bedöma datahanteringsplanerna.[128]

Biblioteken och delar av administrationen bedömer att datahanteringsplanerna kan fungera som ett bra stöd för forskarna. Samtliga tre exempellärosäten erbjuder stöd till forskare för att fylla i planerna.[129] KTH:s bibliotek har diskuterat att slå ihop

---

checklista som under rubriken *Skydda forskningsdata* specifikt nämner informationssäkerhet och informationsklassning, se vidare Svensk nationell datatjänst, *Checklista för Datahanteringsplan*, 2021-01-26.

124 Vetenskapsrådet, ”Ta fram en datahanteringsplan”, hämtad 2023-04-25. I de generella bidragsvillkoren ska medelsförvaltare intyga att en datahanteringsplan kommer att finnas på plats när forskningsprojektet påbörjas och att planen underhålls. Vetenskapsrådet beskriver i en intervju 2023-05-24 att en av anledningarna till att planerna inte begärs in är att de då skulle behöva bedömas som en del av ansökan. Det kräver särskild kompetens som inte finns i nuläget.

125 Intervju LU10.

126 Mejl från företrädare för KTH, 2023-09-13; intervjuer LU8; LU12.

127 Uppsala universitet, ”Datahanteringsplan (DHP)”, hämtad 2023-09-05.

128 Intervju LU16. Vid Karolinska institutet följs datahanteringsplaner upp inom lärosätet. När forskaren fyllt i en plan går den till Forskningsdatastöd som ger feedback och sedan meddelar ansvarig prefekt att planen är på plats. Karolinska institutet, ”Datahanteringsplaner”, hämtad 2023-09-17.

129 Intervjuer BTH7; KTH2; LU8; LU11; LU12; LU24.

processerna att upprätta datahanteringsplan och göra en informationsklassning.[130] Bland de forskare vi intervjuat råder det delade meningar om den praktiska nyttan med dessa planer. De ses ibland som en administrativ börda som inte påverkar hur forskare arbetar med sina data. Det finns också en frustration avseende upplevelsen att ingen ersättning ges för tiden det tar att fylla i en datahanteringsplan och att det råder osäkerheter rörande vad som avses med forskningsdata och vilka krav som ställs på dess hantering.[131]

I EU:s forskningsprogram går det att ansöka om ekonomiskt stöd för kostnader i samband med forskningsdatahantering.[132] Vetenskapsrådet ger inte möjlighet till ekonomisk ersättning för datahantering men hänvisar till att man kan ansöka om sådan finansiering om det direkt kan sägas röra projektet.[133]

Sveriges universitets- och högskoleförbund (SUHF) tog 2018 fram en rekommendation om vad en gemensam nationell mall för en datahanteringsplan bör innehålla. Målsättningen var att möta ”flera aktörers grundläggande behov av dokumentation av forskningsinformation och att förenkla forskarnas administrativa arbete”.[134] Det pågår ett arbete vid många lärosäten att använda datahanteringsplaner som praxis för att FAIR-principerna (se avsnitt 2.6) implementeras i forskningsprojekt redan från början.[135] Svenska universitetsdatanätverket (Sunet) tillhandahåller tjänsten Sunet datahanteringsplan som i november 2023 hade ca 15 lärosäten som kunder.[136] Det finns dock lärosäten som menar att de behöver ha egna planer eftersom den nationella mallen inte passar dem, alternativt att den behöver anpassas.[137]

130 Intervju KTH2.

131 Intervjuer KTH16; KTH17; LU18; LU22; LU21. I EU:s forskningsprogram kan man ansöka om ekonomiskt stöd för kostnader i samband med att hantera forskningsdata.

132 European Commission, *Horizon Europe (HORIZON) Programme Guide,* Version 3.0, 1 April 2023, s. 46–48.

133 Intervju med företrädare för Vetenskapsrådet, 2023-05-24.

134 SUHF, *Reviderad rekommendation för datahanteringsplan*, REK 2018:1 REV, 2019-06-26.

135 SUHF, *Vägledning med åtgärdsförslag för implementering av färdplan för öppen vetenskap. Sammanställning enkät 2023*, SUHF.

136 Mejl från företrädare för Sunet, 2023-11-15. Tjänsten är baserad på datahanteringsverktyget DMPonline från Digital Curation Centre (DCC) vid University of Edinburgh, se Sunet, ”Datahanteringsplan”, hämtad 2023-11-15.

137 Intervju med företrädare för SUHF:s forskningsdatagrupp, 2022-08-23; LU8.

3.3 Separata it-organisationer och egna it-lösningar försvårar ett sammanhållet informationssäkerhetsarbete

Granskningen visar att det finns utmaningar för lärosätena att hitta en bra balans mellan ett generellt it-tjänsteutbud och behovsanpassade lösningar för få eller enskilda forskare. Enskilda institutioner och forskare har många gånger egna it-lösningar, vilket gör det svårare för lärosätena att ha överblick över vilka forskningsdata som hanteras på lärosätet. Det kan i sin tur kan leda till att skyddsvärda forskningsdata inte får ett ändamålsenligt skydd.

3.3.1 Det är vanligt att institutioner och forskare har egna it-lösningar

På alla tre exempellärosäten har det framkommit att det är förhållandevis vanligt att forskare och institutioner har egna lösningar för till exempel datalagring och it-säkerhet, som inte är del av lärosätets gemensamma it-infrastruktur. Det kan till exempel gälla hur data lagras, vilken utrustning som köps in och integreras i lärosätets befintliga it-miljö, vilka externa it-tjänster som används och att egna institutioner sätter upp egna servrar. Både forskare och prefekter som vi intervjuat nämner att de är medvetna om de risker som följer av att skapa egna it-lösningar, exempelvis för datalagring, och att det har uppstått problem med it-säkerhet när anställda väljer egna lösningar.[138]

Det finns exempel på forskare som blir hänvisade av sitt lärosäte att hantera data hos en extern samarbetspartner (till exempel företag eller annat universitet) eftersom det egna lärosätet inte har ändamålsenliga it-lösningar eller säkerhetsåtgärder på plats. Det kan handla om forskningsprojekt som hanterar säkerhetsskyddsklassificerade uppgifter, eller känsliga personuppgifter i form av patientuppgifter.[139]

På vissa håll har lokala lösningar vuxit fram organiskt i decentraliserade organisationer där it-ansvaret och tillhörande it-stöd ligger eller har legat på institutionen. I andra fall har speciallösningar skapats av forskare själva till följd av ett missnöje med befintliga lösningar på central lärosätesnivå. Det finns även exempel på lösningar som har vuxit fram underifrån för att senare bli

138 Intervjuer BTH8; BTH11; BTH13; BTH14; KTH1; KTH5; KTH10; KTH15; KTH18; LU9; LU13; LU16; LU17; LU18; LU20; LU21; LU22; LU29.

139 Intervjuer LU3; KTH9; KTH17.

universitetsövergripande. I vissa fall kan de centrala lösningarna även upplevas som för komplicerade eller kostsamma, och därför väljas bort.[140]
Separata it-organisationer och egna it-lösningar är en konsekvens av att många lärosäten – och särskilt de äldre och större – har en tradition av decentralisering. Det är också en konsekvens av att lärosätena inte har prioriterat informationssäkerhet och datahantering, och därmed inte har tillgodosett forskningsverksamhetens diversifierade behov.

3.3.2 It-förvaltningar på fakultets- och institutionsnivå gör det svårare för funktioner på central lärosätesnivå att identifiera forskares gemensamma behov

Forskare i vår granskning använder alltså ofta både lärosätesövergripande och fakultets- och institutionsgemensamma it-system. De kan samtidigt ha egna it-lösningar, till exempel för att lagra forskningsdata, som inte it-förvaltningarna på olika nivåer känner till. Som en följd blir det svårare för lärosätena att veta vilka data som hanteras i de separata systemen och vilka gemensamma behov som finns av it-tjänster. För att kunna dimensionera säkerhetsåtgärder på ett ändamålsenligt sätt behöver it-organisationerna på lärosätet ha kunskap om vilka forskningsdata som har skyddsvärden, samt vilka behov forskare har i relation till dessa data. Riksrevisionen konstaterar att separata it-system försvårar detta.

Central förvaltning och it-förvaltning uppger att det ofta är önskvärt att så många anställda som möjligt använder samma it-tjänster.[141] Det är kostnadseffektivt och skapar bättre förutsättningar för ett sammanhållet säkerhetsarbete. Genom grundläggande ”it-hygien” i form av exempelvis uppdaterad mjukvara och begränsade administratörsrättigheter, går det att uppnå ett visst mått av säkerhet i den it-miljö som lärosätet använder. Men lärosätens möjlighet till sammanhållen teknisk säkerhet begränsas när separata it-system upprättas. Några av de större lärosätena lyfter lärosätenas storlek, decentraliserade organisationer och it-förvaltningar som de största utmaningarna för att kunna bedriva ett systematiskt informationssäkerhetsarbete.[142] Samtidigt uppfattas inte decentralisering nödvändigtvis som ett problem i sig, utan kan även underlätta mer behovsanpassade lösningar vid institutioner för att hantera skyddsvärda data säkert.[143] Detta behov blir större om man vid lärosätets gemensamma it-avdelning inte tydligt förankrar de system och tjänster som erbjuds hos användarna. Vid

140 Intervjuer BTH12; KTH17; KTH18; LU2; LU13; LU16; LU17; LU18; LU21.
141 Intervjuer KTH5; LU13; LU14; LU27.
142 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.
143 Intervju LU15.

KTH, exempelvis, finns vissa institutioner som har egna it-ansvariga direkt underställda prefekten trots att it-driften ska vara på central lärosätesnivå.[144]

3.4 Lärosätenas riskbedömningar inkluderar sällan informationssäkerhet för forskningsdata

Eftersom många forskare inte klassar sina forskningsdata saknas det tillräckliga underlag för riskbedömningar på institutioner och lärosätesnivå. Informationssäkerhet specifikt rörande forskningsdata inkluderas sällan i riskanalyserna på central lärosätesnivå även om informationssäkerhet tas upp. Dessutom rapporterar lärosätena få it-incidenter. Det kan leda till att lärosätena inte åtgärdar säkerhetsbrister och därmed inte heller inför ändamålsenliga säkerhetsåtgärder.

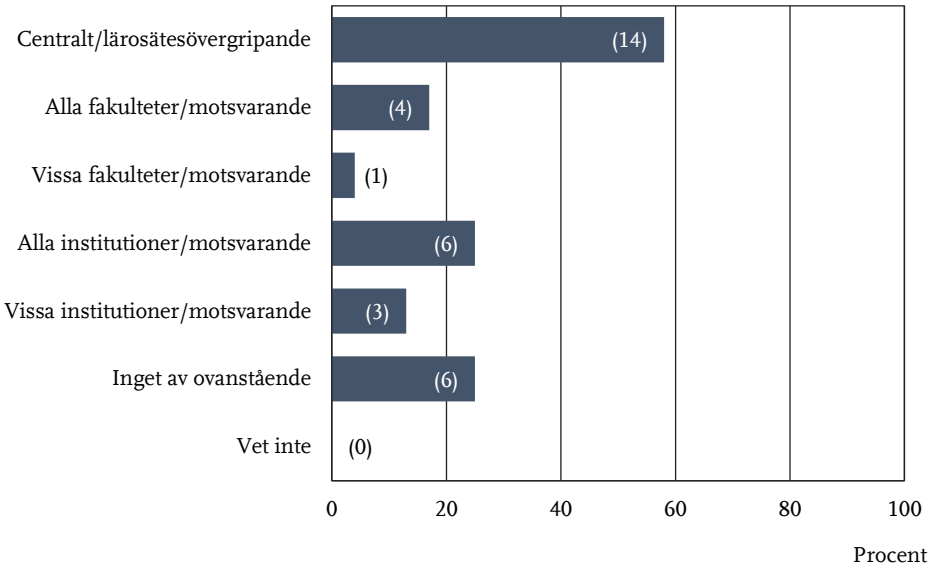
3.4.1 Lärosätena gör riskanalyser på central nivå men informationssäkerhet kopplat till forskningsdata ingår inte alltid

Riskanalyserna på central lärosätesnivå inkluderar inte alltid informationssäkerhet. Det är en brist som även uppmärksammades av Riksrevisionen 2009 och 2010. I Riksrevisionens enkät uppger 14 lärosäten (58 procent) att de årligen genomför och dokumenterar riskbedömning kopplat till *informationssäkerhet* på lärosätesövergripande nivå (se figur 3). Som framgår av figuren är det ovanligt att sådana riskbedömningar görs på fakulteter och institutioner. Vart fjärde lärosäte uppger att det inte görs några organisatoriska riskbedömningar inom informationssäkerhet vid vare sig institutioner, fakulteter eller på lärosätesövergripande nivå.[145]

144 Intervju KTH13.

145 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

Figur 3 Riskbedömning inom informationssäkerhet
Fråga: På vilka organisatoriska nivåer genomförs och dokumenteras en riskbedömning inom informationssäkerhet minst en gång per år?



Källa: Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.
Anm.: Andel som angett respektive nivå, flera nivåer kan anges, antal lärosäten inom parentes.

Knappt hälften av de 24 lärosätena uppger i Riksrevisionens enkät att *forskningsdata* ingår i riskbedömningen inom informationssäkerhet på någon av nivåerna. Det är ett riskområde som på vissa håll saknas helt och hållet, och som i de flesta fall inte beaktas tillräckligt.[146]

Vid de tre exempellärosätena finns informationssäkerhet med i de lärosätesövergripande riskanalyserna och hanteringen av forskningsdata tas upp i viss mån.[147]

Ordningen i riskarbetet är i regel att den centrala lärosätesnivån försöker samla upp risker organisatoriskt genom fakulteter och institutioner. Denna process är särskilt beroende av hur väl prefekterna (eller annan ansvarig på institutionsnivå) samlar upp riskerna från sina medarbetare på institutionen. Vid de tre

146 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

147 Blekinge tekniska högskola, *Riskhantering vid BTH, verksamhetsanalys och riskkostnadsberäkning avseende 2021/2022*; KTH, *KTH:s risker 2022, riskanalys 2021*, 2022-01-17; KTH, *KTH:s riskanalys 2022 – intern styrning och kontroll*, 2023-01-18; Lunds universitet, *Riskarbetet 2022.*

exempellärosätena är det vanligt att prefekter ombeds bidra till fakultetens gemensamma övergripande riskanalys, men informationssäkerhet lyfts inte alltid i de analyserna.[148] Vid LU genomförde Chief Information Security Officer år 2022 organisatoriska riskworkshoppar med fakulteterna på universitetet, med ambitionen att i framtiden även genomföra motsvarande på institutionsnivå.[149] De flesta prefekter vi intervjuat på KTH uppger att de får komma med inspel till den skolgemensamma riskanalysen.[150] Vid BTH uppger vissa prefekter att det görs riskanalyser på institutionsnivå, medan andra säger att det inte görs.[151]

3.4.2 Många risker som löpande identifieras inom olika delar av lärosätena fångas inte upp i det systematiska riskarbetet

Få institutioner på de tre exempellärosätena har en systematisk och formaliserad intern process för att identifiera, analysera och värdera risker som dokumenteras. I intervjuer framkommer att de riskprocesser som är mer formaliserade i första hand rör andra frågor än informationssäkerhet och forskningsdata. Det kan exempelvis handla om kompetensförsörjning, studentrekrytering, forskningsfinansiering, personalsäkerhet, fysiskt skydd, skalskydd, arbetsmiljö, kemikaliehantering och skaderisk i experimentella miljöer. Detta återspeglas också i Riksrevisionens enkät.[152]

Flera lärosäten beskriver i enkäten hur forskare löpande gör riskbedömningar rörande forskningsdata som inte dokumenteras i en samlad organisatorisk riskanalys. Riskbedömningar görs till exempel när datahanteringsplaner och forskningsavtal upprättas samt vid personuppgiftsbehandling. Liknande utsagor om löpande riskbedömningar i det dagliga arbetet framkommer i intervjuer med forskande och administrativ personal på lärosätena.[153] Exempelvis väcks frågeställningar om datalagring och lokalsäkerhet när ett forskningsprojekt inleds. Forskare refererar också till att man löpande gör ”mjukare bedömningar” rörande

148 Intervjuer BTH5; BTH8; KTH9; KTH10; KTH11; KTH13; KTH14; KTH15.

149 Intervju LU1.

150 Intervjuer KTH9; KTH10; KTH11; KTH13; KTH14; KTH15.

151 Intervjuer BTH5; BTH8.

152 Intervjuer BTH5; KTH10; KTH11; KTH14; LU16; LU17; LU26. Vissa lärosäten arbetar dessutom inte med riskanalyser inom informationssäkerhet utifrån organisatoriska enheter, som institutioner, utan istället utifrån t.ex. förvaltningsobjekt, såsom informationssystem; Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

153 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1; intervjuer BTH8; KTH4; KTH10; LU3; LU20.

risk, att man har ett riskminimerande beteende i allmänhet samt att risk är något som det förs diskussioner om men som inte dokumenteras.[154]

3.4.3 Lärosätena rapporterar få informationssäkerhetsincidenter

De flesta lärosäten har system och rutiner för att rapportera informationssäkerhetsincidenter, men det finns skäl att tro att mörkertalet för incidenter är stort. Det är också otydligt vad som skiljer en it-incident från en informationssäkerhetsincident.[155] Det kan bero på att det historiskt varit fokus på it-incidenter. Incidentrapportering är viktig eftersom den utgör underlag för framtida säkerhetsåtgärder. När incidenter inte rapporteras kan det innebära att säkerhetsbrister inte åtgärdas.

Rapporteringsplikt för it-incidenter framgår både i MSB:s föreskrifter och i säkerhetsskyddsförordningen (2021:955). Det finns däremot inget krav på att rapportera informationssäkerhetsincidenter i MSB:s föreskrifter. I säkerhetsskyddsförordningen (2021:955) finns dock en anmälningsplikt bland annat om det finns skäl att anta att en säkerhetsskyddsklassificerad uppgift otillåtet har röjts.[156]

I MSB:s självskattningsverktyg Infosäkkollen 2021 rapporterade 10 lärosäten och forskningsinstitut att de upptäckt mellan 2 och 664 informationssäkerhets-incidenter de senaste två åren. De flesta rapporterade knappt 10 incidenter.[157] Att så få rapporterat informationssäkerhetsincidenter och den stora variationen tyder på stora skillnader i hur lärosätena tolkar vad som ska rapporteras.

Riksrevisionens intervjuer vid de tre exempellärosätena bekräftar bilden av att det finns brister i kännedomen om vad en informationssäkerhetsincident är, vilka incidenter som ska rapporteras och hur de ska rapporteras. Dessutom saknas ändamålsenliga system för att rapportera informationssäkerhetsincidenter. Vid BTH och LU finns system för att rapportera *it-incidenter* och vid KTH görs rapporteringen via pdf-mallar.[158]

---

154 Intervjuer BTH12; BTH13; KTH4; KTH10; KTH17; LU19.

155 It-incidenter utgör dock rimligen den absolut största delen av inträffade informationssäkerhetsincidenter eftersom den mesta informationen hanteras i it-system.

156 MSB:s föreskrifter om rapportering av it-incidenter för statliga myndigheter (MSBFS 2020:8); 2 kap. 4 § säkerhetsskyddsförordningen (2021:955). År 2022 rapporterades 330 it-incidenter till MSB, varav 231 rapporterades av myndigheter. Totalt 69 myndigheter rapporterade minst en incident vardera, se MSB, 2022a, s. 16.

157 Genomgång av underlag till MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen, Resultatredovisning Infosäkkollen 2021*, 2022b, 2022-08-26.

158 Intervjuer BTH1; BTH8; BTH13; KTH1; LU2.

Av Riksrevisionens enkät framgår att 18 av 24 lärosäten, det vill säga 75 procent, har ett centralt incidentrapporteringssystem som inkluderar alla typer av incidenter. De allra flesta lärosäten har också rutiner för hur informationssäkerhetsincidenter ska hanteras och dokumenteras, samt rapporteras. Något färre har rutiner för hur de ska identifieras och bedömas samt följas upp (14 respektive 15 av 24).[159]

[159] Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

4 Lärosätenas utformning av informationssäkerhetsarbetet

I det här kapitlet besvarar vi frågan om huruvida universitet och högskolor har utformat informationssäkerhetsarbetet på ett effektivt sätt för att hantera skyddsvärda forskningsdata. Nedan sammanfattar vi våra huvudsakliga iakttagelser.

4.1 Riksrevisionens huvudsakliga iakttagelser

- Flera lärosäten håller på att bygga upp eller revidera sina ledningssystem för informationssäkerhet. Policydokument och riktlinjer finns på plats, men de är inte alltid aktuella. Många lärosäten anger resursbrist och flera har vakanser i organisationen som ska arbeta med informationssäkerhet.
- Roll- och ansvarsfördelning för informationssäkerhetsarbetet är ofta otydlig, vilket försvårar arbetet. Den funktion som är ansvarig för att samordna informationssäkerhetsarbetet är placerad på it-avdelningen på nästan hälften av de 24 lärosätena i granskningen. Det kan försvåra den strategiska och kravställande som rollen behöver ha. Informationssäkerhetsansvariga rapporterar inte heller alltid till rektor eller styrelse.
- Medarbetarnas kompetens inom informationssäkerhet varierar stort, men är överlag inte tillräcklig. Det finns begränsad kunskap om vilken typ av forskningsdata som kan vara skyddsvärd och vilka regelverk som reglerar hanteringen. Få medarbetare har gått de utbildningar som erbjuds i informationssäkerhet. Det är otydligt för lärosätena vad som ska ingå i den bakgrundskontroll som enligt MSB:s föreskrifter ska göras av personal som en av flera åtgärder för att säkerställa att information behandlas på ett säkert sätt.
- Lärosätena erbjuder stöd för korrekt hantering av forskningsdata, men det utnyttjas inte i så hög utsträckning av forskare. Viktiga stödfunktioner är inte tillräckligt samordnade och når inte alltid ut till de forskare som behöver stöd. Vidare saknas stöd för att hantera forskningsdatas hela livscykel eftersom det finns brister i såväl riktlinjer som det tekniska stöd som lärosätena kan erbjuda forskare för lagring och långsiktigt bevarande av forskningsdata.

4.2 Styrningen av informationssäkerhetsarbetet har brister

Granskningen visar att många lärosäten håller på att bygga upp en organisation, eller revidera befintlig, för att styra informationssäkerhetsarbetet. Centrala styrdokument är inte alltid uppdaterade. Flera lärosäten uppger att de har svårt att rekrytera personal med kompetens inom informationssäkerhetsområdet.

4.2.1 Flera lärosäten har varit senfärdiga i implementeringen av ett ledningssystem för informationssäkerhet

Trots att det funnits föreskriftskrav sedan 2008 finns det lärosäten som anger att de håller på att bygga upp eller införa nya ledningssystem för informationssäkerhet, vad gäller både dokumentation och organisation.[160]

Redan 2003 kritiserade internrevisionen institutionerna vid Lunds universitet (LU) för bristande informationssäkerhet. Internrevisionen kopplade många av de konstaterade bristerna till lärosätets decentraliserade organisation och kraven på öppenhet. Som svar angav LU bland annat att man skulle inleda ett arbete med att ta fram ett ledningssystem för informationssäkerhet.[161] I Riksrevisionens granskning 2010 framkom fortsatta brister och LU påbörjade då en universitetsövergripande process med att återigen upprätta ett ledningssystem för informationssäkerhet.[162] I internrevisionens granskning 2014 av styrning av informationssäkerhet var slutsatsen bland annat att det fanns behov av ytterligare riktlinjer och att gällande styrdokument inte tillämpades fullt ut på fakultets- och institutionsnivå.[163] 2017 fattade rektor beslut om reviderade riktlinjer för informationssäkerhet.[164] 2019 påbörjades arbetet på nytt med att bygga upp ett heltäckande ledningssystem för informationssäkerhet.[165] I en uppföljning samma

160 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1. Internrevisionen vid flera lärosäten konstaterar detsamma.

161 Lunds universitet, Internrevisionen, *Årsrapport från internrevisionen år 2003*, 2004-02-06; Lunds universitet, Förvaltningschefen, *Kommentar till årsrapport från internrevisionen 2003*, 2004-02-11.

162 Riksrevisionen, *Granskning av intern styrning och kontroll av informationssäkerheten vid Lunds universitet*, 2010-01-22; Lunds universitet, *Svar på revisionsrapport 2010-01-22 granskning av intern styrning och kontroll av informationssäkerheten vid Lunds universitet*, 2010-04-21.

163 Lunds universitet, Internrevisionen, *Styrning av informationssäkerhet*, 2014-06-19, s. 8.

164 Lunds universitet, *Riktlinjer för informationssäkerhet vid Lunds universitet*, 2017-06-22.

165 Intervjuer LU1; LU2; LU3; LU7.

år konstaterades att flertalet av internrevisionens rekommendationer genomförts.[166] I mars 2022 fastställde rektor ett ledningssystem för informationssäkerhet.[167]

Även vid Kungl. Tekniska högskolan (KTH) har internrevisionen återkommande fört fram brister i lärosätets informationssäkerhetsarbete. 2014 rekommenderade internrevisionen KTH att implementera ett ledningssystem för informationssäkerhet.[168] 2020 konstaterade internrevisionen att KTH:s ledningssystem för informationssäkerhet i flera avseenden inte uppfyllde kraven trots ett arbete som pågått under ett antal år. Vid KTH integrerades it- och informationssäkerhetsarbetet på den centrala it-avdelningen 2017 och en ny roll som chef för it- och informationssäkerhet inrättades.[169] I april 2023 rekryterade KTH en säkerhetschef som fått i uppdrag att bygga upp en helt ny säkerhetsorganisation på lärosätet. Bland annat rekryteras en informationssäkerhetsspecialist under hösten 2023.[170]

Riksrevisionens granskning av informationssäkerhet vid Blekinge tekniska högskola (BTH) 2009 visade att väsentliga riktlinjer som bör finnas i ett ledningssystem för informationssäkerhet saknades, bland annat riktlinjer för informationsklassning, riskanalys och incidenthantering.[171] I sitt svar till Riksrevisionen meddelade rektor att högskoldirektören fått i uppdrag att bland annat utveckla befintliga policyer och riktlinjer till en säkerhetspolicy.[172] Informationssäkerhetspolicyn upprättades 2010 och har inte reviderats sedan dess, men arbete pågick under våren 2023 med att uppdatera den, bland annat gällande begrepp.[173]

166 Lunds universitet, *Uppföljning av Yttrande över Internrevisionens rapport "Styrning av informationssäkerhet"*, 2019-10-11.

167 Lunds universitet, *Ledningssystem för informationssäkerhet vid Lunds universitet*, 2022-03-24.

168 Ernst & Young, *Granskning av informationssäkerhet på KTH*, juni 2004; KTH, Internrevisionen, *Arbetet med informationssäkerhet vid KTH*, Internrevisionsrapport 1/2014, 2014-10-17.

169 KTH, Internrevisionen, *Granskning av KTH:s ledningssystem för informationssäkerhet*, Revisionsrapport 1/2020, 2020-10-01.

170 KTH, "Så bygger hon KTH:s nya säkerhetsavdelning", hämtad 2023-08-27; KTH, "Lediga jobb, CISO - informationssäkerhetsspecialist till KTH", hämtad 2023-09-10.

171 Riksrevisionen, *Granskning av intern styrning och kontroll av informationssäkerheten vid Blekinge tekniska högskola 2009*, 2010-01-26.

172 Blekinge tekniska högskola, *Information med anledning av Riksrevisionens rapport "Granskning av intern styrning och kontroll av informationssäkerheten vid Blekinge tekniska högskola 2009"*, 2010-03-01.

173 Intervju BTH1.

4.2.2 Styrdokument inom informationssäkerhet är inte alltid uppdaterade

Samtliga 24 lärosäten i vår granskning har en informationssäkerhetspolicy eller motsvarande, men de uppdateras i olika omfattning: ibland sällan och i vissa fall inte alls. Hälften av policyerna upprättades 2018 eller senare och de flesta lärosäten anger att de reviderades 2021 eller 2022. 2 lärosäten upprättade sin policy 2010 respektive 2014 utan att ha reviderat dem sedan dess. I några fall är centrala dokument för informationssäkerhet fortfarande under framtagande.[174] I knappt hälften av informationssäkerhetspolicyerna anges rektor som ytterst ansvarig.[175] När styrdokument som informationssäkerhetspolicyer är inaktuella riskerar de att tappa i relevans och därmed inte fungera styrande som avsett. Dessutom riskerar kunskapen om dem i organisationerna att vara låg.

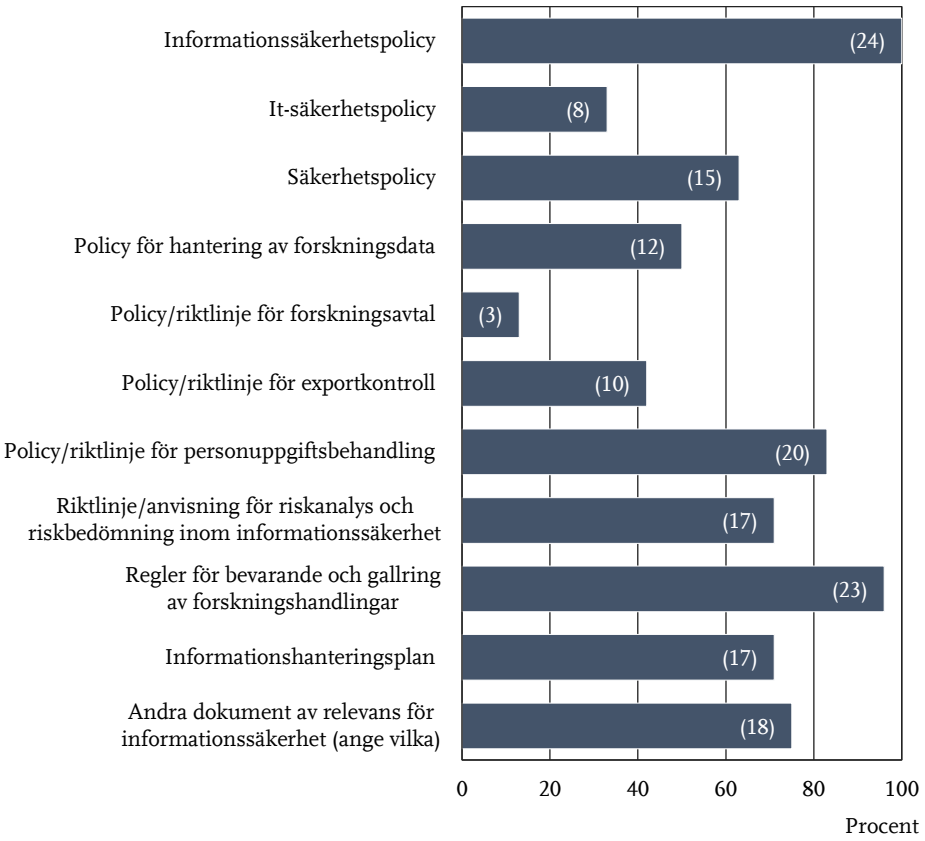
Andra styrdokument utöver informationssäkerhetspolicyer som förekommer är regler för bevarande och gallring av forskningshandlingar, delegationsordningar, riktlinjer för olika administrativa processer, juridiska riktlinjer för forskningssamarbeten, säkerhetspolicyer, avtal rörande internationalisering och styrdokument för gallring, se figur 4.[176] Riksrevisionen konstaterar att mängden styrdokument av relevans för informationssäkerhet och forskningsdatahantering kan göra det svårare för medarbetare att hitta rätt information för den praktiska hanteringen av forskningsdata.

174 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

175 Riksrevisionens sammanställning av 24 lärosätens informationssäkerhetspolicyer/motsvarande.

176 Riksrevisionens sammanställning av 24 lärosätens informationssäkerhetspolicyer/motsvarande; Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1. Andra dokument av relevans för informationssäkerhetsarbetet (som 75 procent av lärosätena anger att de har) är t.ex. mejl- och lösenordsregler, styrdokument inom it och it-säkerhet, datahanteringsplaner, upphandlingskrav, rutiner för exportkontroll, rutiner för personuppgiftsbehandling etc.

Figur 4 Upprättade styrdokument inom informationssäkerhet och forskningsdatahantering vid de 24 lärosätena



Källa: Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.
Anm.: Andel som upprättat respektive styrdokument, antal lärosäten inom parentes.

4.2.3 Informationssäkerhetsarbetet konkurrerar med andra mål i forskningsverksamheten

Granskningen visar att det inte alltid är tydligt för lärosätena hur frågan om informationssäkerhet för forskningsdata ska hanteras i relation till andra mål, som exempelvis internationalisering och öppen vetenskap. Flera lärosäten menar att regelverk står i konflikt med varandra och att det kan vara svårt att prioritera.[177] Det finns en uppfattning att informationssäkerhet och skydd av forskningsdata handlar om kostsamt administrativt extraarbete, som därmed får lägre prioritet i konkurrens med andra frågor. Uppfattningen finns också att det övergripande

[177] Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

målet är att tillgängliggöra data och att utmaningen snarare handlar om externa samarbetspartners önskemål om att hålla information konfidentiell.[178]
I Vetenskapsrådets årliga kartläggning av arbetet med öppen tillgång till forskningsdata framkommer att det finns en osäkerhet bland forskare hur man ska hantera frågor om integritet, etik, säkerhet och GDPR, stora datamängder och kvalitativa data.[179]

Vidare menar många lärosäten att det är svårt att följa MSB:s föreskrifter eftersom verksamheten skiljer sig från den vid många andra myndigheter, bland annat i fråga om stora och diversifierade datamängder med krav på öppenhet och tillgängliggörande.[180] Enligt MSB har lärosätena många gånger utvecklat system på ad hoc-basis utan att ha föreskrifterna i åtanke, trots att de funnits sedan 15 år. Det har fått till följd att det på många håll krävs ett stort omtag vad gäller exempelvis it-lösningar vid lärosätena för att leva upp till föreskriftskraven.[181]

4.2.4 Många lärosäten anger resursbrist för informationssäkerhetsarbetet

Granskningen visar att lärosätena generellt anser att de saknar resurser för att bedriva ett tillräckligt bra informationssäkerhetsarbete. Flera lärosäten anger att de har pågående rekryteringar inom området.

60 procent av lärosätena kan inte ange hur mycket personalresurser eller finansiella resurser som budgeterades 2023 för informationssäkerhet på central lärosätesnivå.[182] Av de 11 som svarat anges belopp mellan 1,6 och 8,9 miljoner kronor. I enkätsvaren framträder ingen tydlig relation mellan resurser och storlek på lärosäte. Två mindre högskolor anger det högsta respektive lägsta beloppet. Ett universitet pekar på svårigheten att ange ett belopp eftersom man har som ambition att integrera informationssäkerhetsarbetet i övrig verksamhet. Exempelvis inkluderar inte lärosätet kostnaderna för representanter i arbetsgruppen för

178 Intervjuer BTH3; BTH7; KTH2; KTH8; LU2; LU5, LU10; LU22; LU23.

179 Vetenskapsrådet, *Öppen tillgång till forskningsdata 2023. En kartläggning, analys och bedömning*, 2023, s. 19.

180 Intervjuer BTH5; BTH10; KTH5; KTH, KTH:s remissvar *Förslag till MSB:s föreskrifter om informationssäkerhet och föreskrifter om it-säkerhet för statliga myndigheter,* 2020-02-11; It-säkerhetsnätverket, *Sektorsgemensam återkoppling Vägledning säkerhetsåtgärder i informationssystem v. 0.2,* 2022-04-13.

181 Intervju med företrädare för MSB, 2023-06-09. Som diskuteras i 4.2.1 har bristerna att efterleva föreskriftskraven påtalats i många internrevisionsrapporter under en längre tid.

182 Det inkluderar personalkostnader i form av löner inklusive konsulter, projektkostnader, kurser, utbildningar, seminarier och säkerhetsåtgärder (till exempel it-tjänster) vars primära syfte är att förbättra informationssäkerheten, se Riksrevisionens enkät om informationssäkerhet, del 1.

dataskydd och forskningskoordinatorer i it- och datahantering, även om deras arbete till stor del relaterar till informationssäkerhet. Flera lärosäten anger att de kommer tillsätta resurser framöver för bland annat utveckling av ledningssystem för informationssäkerhet.[183]

Sex lärosäten nämner specifikt att de har vakanser inom informationssäkerhetsområdet. Flera lärosäten uppger att de har svårt att rekrytera och behålla medarbetare med rätt kompetens inom informationssäkerhetsområdet. Några anledningar som uppges är brist på tillräckligt kompetenta sökande och att de inte kan konkurrera lönemässigt med den privata sektorn.[184] I intervjuer framkommer att LU har haft svårt att anlita informationssäkerhetskonsulter. Medarbetare med centrala roller har också avslutat sina tjänster efter kort tid.[185] Vid KTH har det nyligen anställts en säkerhetschef efter att tjänsten varit vakant en längre period.[186] Vid BTH är vissa roller som är centrala för informationssäkerhetsarbetet deltidstjänster.[187]

4.3 Roll- och ansvarsfördelning för informationssäkerhetsarbetet är ofta otydlig

Riksrevisionens granskning visar att det råder oklarheter i forskningsverksamheterna om vem som är ansvarig för informationssäkerheten. Det kan vara en särskild utmaning när ansvaret finns inom såväl förvaltning och verksamhetsstöd som i den akademiska organisationen. Funktionen som ansvarar för att driva och samordna arbetet med informationssäkerhet är ofta placerad på it-avdelningen, vilket kan försvåra möjligheten att arbeta strategiskt eftersom det ingår i rollen att vara granskande och kravställande. Dessutom rapporterar informationssäkerhetsansvariga inte heller alltid regelbundet till rektor eller styrelse.

183 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.
184 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.
185 Intervjuer LU2; LU24; telefonsamtal med CISO Lunds universitet, 2023-08-08.
186 Intervjuer KTH1; KTH5; KTH, ”Så bygger hon KTH:s nya säkerhetsavdelning”, hämtad 2023-06-13.
187 Intervjuer BTH1; BTH3.

4.3.1 Informationssäkerhetschef rapporterar inte alltid till rektor eller styrelse

Granskningen visar att det varierar vem informationssäkerhetschef/motsvarande[188] rapporterar till. 10 lärosäten uppger att de har en formaliserad återkommande rapportering mellan informationssäkerhetschef och rektor eller styrelse. 4 lärosäten anger att ingen reglerad rapportering från informationssäkerhetschef sker över huvud taget.[189]

Att ledningen håller sig informerad om informationssäkerhetsarbetet är en förutsättning för att den ska kunna fatta informerade beslut. I regeringens beslut om att se över sammansättningen av lärosätenas styrelser framhålls att säkerhetspolitisk kompetens behöver finnas i styrelsen.[190] Riksrevisionen gör ingen bedömning av ändamålsenligheten i regeringens beslut. Vi konstaterar dock att det är avgörande för ett framgångsrikt säkerhetsarbete att erforderlig kompetens och expertis finns i den operativa verksamheten och att kommunikation och samarbete mellan ledningen och säkerhetsansvariga är god.

Enligt MSB behöver informationssäkerhetschefens strategiska funktion vara åtskild från organisationens interna it-produktion eftersom rollen ska vara kravställande och granskande gentemot denna.[191] Av vår enkät framgår att knappt hälften av informationssäkerhetscheferna har sin placering på it-avdelningen. Andra organisatoriska placeringar är rektors kansli, förvaltningschefs stab/motsvarande, säkerhetsavdelningen, enheten för digital utveckling och styrning och avdelningen för infrastruktur. Vid 4 lärosäten innehas rollerna informationssäkerhetschef och it-säkerhetschef av samma person.[192]

Organisationen vid de tre exempellärosätena visar på variationen i informationssäkerhetschefens ansvar och placering. KTH har en it-säkerhetschef som också ansvarar för att samordna informationssäkerhetsarbetet, med en lång

---

188 Om informationssäkerhetschef inte finns avses istället informationssäkerhetsspecialist, informationssäkerhetssamordnare, informationssäkerhetsstrateg eller motsvarande, se Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

189 Med reglerad rapportering avses en formaliserad rutin som är regelbundet återkommande. 12 lärosäten uppger i sina enkätsvar att de har en informationssäkerhetschef/motsvarande och 18 att de har en informationssäkerhetssamordnare. 2 lärosäten uppger att inte har någon sådan befattning, men att de har en arbetsgrupp för informationssäkerhet, se Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

190 Utbildningsdepartementet, ”Pressmeddelande: Nya styrelser för 30 universitet och högskolor”, 2023-04-27, hämtad 2023-09-17.

191 MSB:s metodstöd för systematiskt informationssäkerhetsarbete, informationssäkerhet.se, ”Utforma, CISO-rollens organisatoriska placering”, hämtad 2023-09-19.

192 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

bakgrund vid lärosätets it-avdelning.[193] Vid LU innehas befattningen Chief Information Security Officer sedan 2019 av en externrekryterad person med bakgrund i näringslivet. Funktionen är placerad vid rektors stab.[194] Vid BTH är informationssäkerhetsansvarig placerad under högskoledirektören. Rollen är ett deltidsuppdrag på 40 procent vid sidan av ordinarie tjänst som ekonom. Uppdraget gavs muntligt 2018.[195]

I den rådgivningstjänst som MSB tillhandahåller sedan 2022 kommer det in frågor från lärosäten bland annat om kategorisering av informationstyper och tekniska säkerhetsåtgärder. Utöver det anger MSB att återkommande frågor från lärosätena handlar om att informationssäkerhetschef/motsvarande önskar stöd för att komma vidare i sitt arbete. Informationssäkerhetschefer vid lärosätena upplever enligt MSB att det är svårt att nå fram till ledningen och få förståelse för informationssäkerhetsarbetet. Det förekommer också att it-chefer kontaktar MSB direkt för stöd att tolka föreskrifter utan att först ha kontaktat informationssäkerhetsansvarig på lärosätet.[196]

Inom det statliga nätverket för informationssäkerhet (Snits) har det förekommit diskussioner om huruvida lärosätena ska utgöra en egen grupp. MSB uppger att de som deltar i nätverket för lärosätenas räkning snarare arbetar med it-drift än har en informationssäkerhetsfunktion. Det påverkar vilken möjlighet de har att ta sig an rollen som strategisk och samordnande funktion.[197]

4.3.2 Det finns olika uppfattningar om vem som är ansvarig för informationssäkerheten på institutionerna

Granskningen visar att prefekter ser olika på sitt ansvar och att det förekommer olika uppfattningar om vem som är formellt ansvarig för informationssäkerheten på institutionerna. Det kan försvåra implementeringen av ett systematiskt informationssäkerhetsarbete.

Riksrevisionen konstaterar att både akademiska och administrativa högre chefer samt informationssäkerhetsmedarbetare ofta utgår från att prefekter för vidare information till institutionernas forskare om säker hantering av forskningsdata i

193 Intervju KTH1.

194 Intervjuer LU1; LU2.

195 Intervjuer BTH1; BTH3.

196 Mejl från företrädare för MSB med svar på kompletterande frågor från Riksrevisionen om informationssäkerhet vid UoH, 2023-06-30.

197 Mejl från företrädare för MSB med svar på kompletterande frågor från Riksrevisionen om informationssäkerhet vid UoH, 2023-06-30.

enlighet med styrdokument.[198] Granskningen visar dock att prefekter har varierande kunskap om informationssäkerhet och ser olika på sitt uppdrag och sitt ansvar för informationssäkerhet. Flera prefekter anger att de litar på att forskarna gör rätt och att forskarna själva lyfter informationssäkerhetsfrågor till prefektnivå om och när de uppstår. Prefekter ser sig ofta som ansvariga men framhåller att ett stort ansvar även ligger på medarbetarna, och att relationen bygger på ett förtroende dem emellan.[199]

Riksrevisionen konstaterar att prefektens uppdrag som tillfälligt och ofta kollegialt tillsatt kan försvåra såväl kontinuitet som viljan att agera som en överordnad, exempelvis vid uppföljning av efterlevnaden av informationssäkerhetsarbetet. Vidare kan uppdragets tidsbegränsning medföra en avsaknad av ägarskap för frågan. Riksrevisionen konstaterar vidare att frågor om informationssäkerhet inte alltid är inkluderade i lärosätenas delegations- och arbetsordningar.[200] Dessutom kan det variera vem som anges som informationsägare; ofta anges prefekt, forskningsledare, föreståndare för forskningscentrum eller chef över ett område.[201]

Vid KTH finns inte informationsägare med som begrepp i anvisningen för informations- och it-säkerhet, men det framgår att ansvaret för informationssäkerheten ligger hos de verksamhetsansvariga, dvs. skolcheferna. Vid varje skola ska det finnas en ansvarig för informationssäkerheten.[202] På vissa skolor delegeras detta ansvar till prefekter, som i sin tur kan delegera vidare till forskargrupper. På en annan skola ser skolchefen sig själv som operativt ansvarig. Ytterligare en annan skola har inte utsett formellt ansvariga, utan ansvaret har istället informellt delegerats till prefekter och administrativa chefer.[203] Från centralt håll har skolornas administrativa chefer setts som ansvariga på respektive skola,

198 Intervjuer BTH1; BTH2; BTH3; KTH2; KTH4; KTH6; KTH14; LU2; LU4; LU26.

199 Intervjuer BTH5; BTH8; KTH9; KTH10; KTH13; KTH14; KTH15; LU3; LU13; LU16; LU17; LU25.

200 Se Blekinge tekniska högskola, *Arbetsordning för Blekinge tekniska högskola*, 2022-10-01; Blekinge tekniska högskola, *Rektors delegationsordning Blekinge tekniska högskola*, 2021-02-10; Lunds universitet, *Arbetsordning för Lunds universitet,* 2022-10-28 ; Lunds universitet, *Föreskrifter om fördelning av beslutsbefogenheter inom universitetsförvaltningen,* 2021-05-11*;* Lunds universitet, *Lunds universitets föreskrifter om fördelning av beslutsbefogenheter och rätt att teckna avtal vid Lunds universitet,* 2022-06-09. Vid KTH tas informationssäkerhet upp i KTH, *Delegationsordning för KTH*, gäller från och med 2023-01-01 och i KTH, *Arbets- och delegationsordning för verksamhetsstödet vid KTH,* ändrad från och med 2023-01-01. I KTH, *Arbetsordning vid KTH,* senast ändrad från och med 2023-01-01, nämns inte informationssäkerhet specifikt men hänvisning görs till ”KTH:s informationshanteringsplan och andra styrdokument om dokumenthantering”.

201 Se t.ex. Umeå universitet, ”Informationssäkerhet”, hämtad 2023-09-08; Högskolan i Borås, *Ansvar och roller i ledningssystem för Informationssäkerhet (LIS) vid Högskolan i Borås*, 2022-05-04.

202 KTH, *Anvisning för informations- och IT-säkerhet,* 2014-02-01.

203 Intervjuer KTH4; KTH6

men det är inte ett ansvar som de har tilldelats formellt.[204] Internrevisionen vid KTH konstaterade 2020 brister i KTH:s informationssäkerhetsarbete, bland annat gällande otydligheter i ledningens ansvar och att nödvändiga befogenheter inte var tilldelade för berörda roller.[205]

LU använder begreppet informationsriskägare.[206] Där är chefer ansvariga för informationssäkerheten inom det egna ansvarsområdet.[207] LU:s interna analyser har dock visat att chefer på olika fakulteter har olika uppfattning om vem som är ansvarig, men att det är vanligt att prefekten anses vara det.[208] Informationssäkerhetsansvaret nämns dock inte i lärosätesövergripande delegationsordningar eller arbetsordningar.[209]

På BTH är respektive arbetsenhetschef ansvarig för informationssäkerheten inom sin verksamhet. För institutioner innebär det prefekten.[210] Vid intervjuer framkommer att det även finns en uppfattning att det är på den enskilda forskaren som ansvaret vilar.[211] Inte heller vid BTH nämns informationssäkerhet i delegations- eller arbetsordningar.[212]

4.4 Medarbetarnas kompetens inom informationssäkerhet med fokus på forskningsdata varierar stort

Granskningen visar att graden av kompetens och kunskap om informationssäkerhet varierar stort inom lärosätena. Det finns otillräcklig kunskap om vad som kan utgöra skyddsvärda data och vilka åtgärder som behövs för att begränsa åtkomsten. De utbildningsinsatser som lärosätena genomför får inte tillräckligt genomslag bland forskarna. Det kan få till följd att skyddsvärda forskningsdata inte hanteras korrekt.

---

204 Intervju KTH1.

205 KTH, Internrevisionen, *Granskning av KTH:s ledningssystem för informationssäkerhet*, Revisionsrapport 1/2020, 2020-10-01.

206 Lunds universitet, *Ledningssystem för informationssäkerhet vid Lunds universitet*, fastställd av rektor 2022-03-24.

207 Lunds universitet, *Riktlinjer för informationssäkerhet vid Lunds universitet*, 2017-06-22.

208 Intervju LU2.

209 Lunds universitet, *Arbetsordning för Lunds universitet*, 2022-10-28; Lunds universitet, *Föreskrifter om fördelning av beslutsbefogenheter inom universitetsförvaltningen vid Lunds universitet*, 2021-05-11; Lunds universitet, *Lunds universitets föreskrifter om fördelning av beslutsbefogenheter och rätt att teckna avtal vid Lunds universitet*, 2022-06-09.

210 Blekinge tekniska högskola, *Riktlinjer för informationssäkerhet vid Blekinge Tekniska Högskola*, version 1.0, 2012-06-19.

211 Intervjuer BTH6; BTH8.

212 Blekinge tekniska högskola, *Arbetsordning för Blekinge tekniska högskola*, 2022-10-01; Blekinge tekniska högskola, *Rektors delegationsordning, Blekinge tekniska högskola*, 2021-02-10.

4.4.1 Det finns begränsad kunskap om vilken typ av forskningsdata som kan vara skyddsvärd

Det finns överlag en begränsad kunskap om vilken typ av forskningsdata som kan vara skyddsvärd, både bland forskare och andra anställda, liksom att åtkomsten till sådan information kan behöva begränsas från obehöriga. Enligt Säkerhetspolisen har lärosätena bristande kompetens att bedöma vad som är skyddsvärt.[213] Även vid lärosätena finns uppfattningen att det saknas tillräcklig kompetens för att göra de bedömningarna.[214]

16 av 24 lärosäten uppger i vår enkät att de har kartlagt vilka rättsliga krav och andra externa krav som påverkar hanteringen av forskningsdata.[215] Det är vanligt att forskare tänker i första hand på personuppgifter som skyddsvärda forskningsdata, men även andra aspekter vägs in vid bedömningen.[216] Det kan enligt Riksrevisionen bero på uppmärksamheten kring dataskydd och de rättsliga skärpningarna som följde av införandet av den nya dataskyddsförordningen.

Även om man som forskare kan sitt forskningsfält uppger forskare i våra intervjuer att det kan vara svårt att bedöma skyddsvärden eller möjliga framtida användningsområden för ens forskning.[217] Ytterligare en försvårande omständighet är att vissa forskningsdata har låga skyddsbehov separat, men tillsammans med annan information uppstår skyddsvärden och förhöjda skyddsbehov. Exempel på det kan vara vissa dataset som innehåller koordinater, vilket i kombination med andra databaser kan härledas till specifika markägare.[218] Det är också något som Myndigheten för digital förvaltning lyfter som en risk vid tillgängliggörande av information som öppna data.[219] Även externa förutsättningar, som till exempel hotbilder, kan förändra skyddsbehov under forskningsprojektets gång. I KTH:s och LU:s modeller för informationsklassning finns det ingen vägledning för hur forskningsdatas livscykel ska beaktas.[220]

---

213 Intervju med företrädare för Säkerhetspolisen, 2023-03-24.

214 Intervjuer BTH3; BTH10; LU13; LU25.

215 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

216 Intervjuer BTH5; BTH6; KTH4; KTH6; KTH9; KTH10; KTH18; LU17; LU19.

217 Intervjuer BTH11; KTH9; LU19.

218 Intervjuer BTH7; KTH2; KTH5; LU1; LU11.

219 Myndigheten för digital förvaltning, ”Vägledning för att tillgängliggöra information”, hämtad 2023-09-15.

220 KTH, *Anvisning Informationsklassificering för KTH*, riktlinje gäller från och med 2015-01-01; Lunds universitet, *Riktlinjer för informationssäkerhet vid Lunds universitet*, 2017-06-22. Riksrevisionen har inte tagit del av Blekinge tekniska högskolas informationsklassningsmodell.

4.4.2 Lärosätena tycker att det är svårt att bedöma vad som faller under regelverket om säkerhetsskydd

Det är verksamhetsutövarna, i det här fallet lärosätena, som själva ska utreda behovet av säkerhetsskydd om de till någon del bedriver säkerhetskänslig verksamhet.[221] I granskningen framkommer att lärosätena tycker att det kan vara en utmaning att göra den bedömningen. Granskningen visar att lärosätena gör olika bedömningar av likvärdiga verksamheter och information när det gäller säkerhetsskydd. Exempelvis har två lärosäten av liknande storlek och med samma forskningsbredd gjort olika bedömningar. Sammantaget ger våra iakttagelser en bild av att flera lärosäten inte vet om de hanterar säkerhetsskyddsklassificerade uppgifter eller inte. Riksrevisionen konstaterar att det kan leda till att sådana uppgifter eller säkerhetskänslig verksamhet i övrigt inte får tillräckligt skydd.

2 lärosäten uppger i Riksrevisionens enkät att de inte vet om de hanterar säkerhetsskyddsklassificerade uppgifter och 4 lärosäten att de inte vet om de bedriver verksamhet som i övrigt behöver ett säkerhetsskydd. 8 av 24 lärosäten uppger att de hanterar säkerhetsskyddsklassificerade uppgifter. Det är däremot 9 lärosäten som har anmält till sin tillsynsmyndighet att de bedriver verksamhet som faller under säkerhetsskyddslagen. Det är till viss del inte samma lärosäten som svarat ja i enkäten respektive anmält till sin tillsynsmyndighet.[222] Endast 4 lärosäten uppger i vår enkät att de har en beslutad säkerhetsskyddsplan, vilket är ett krav om verksamhetsutövaren i säkerhetsskyddsanalysen kommer fram till att den bedriver verksamhet som faller under säkerhetsskyddslagen.[223]

Om en verksamhet hanterar uppgifter eller bedriver verksamhet som faller under säkerhetsskyddslagen är säkerhetsskyddsåtgärder inte frivilliga. Beroende på vad som framkommer i säkerhetsskyddsanalysen kan det finnas lagkrav på

---

221 2 kap. 1 § säkerhetsskyddslagen (2018:585).

222 Riksrevisionen noterar att det är 2 lärosäten som i Riksrevisionens enkät uppger att de hanterar säkerhetsskyddsklassificerade uppgifter som inte anmält detta till sin tillsynsmyndighet. Omvänt så är det 4 lärosäten som anmält till sin tillsynsmyndighet att de bedriver verksamhet som omfattas av säkerhetsskyddslagen, men som i Riksrevisionens enkät inte uppgav att de hanterar säkerhetsskyddsklassificerade uppgifter. 13 av 24 lärosäten uppger i Riksrevisionens enkät att de har en säkerhetsskyddschef, vilket är ett krav om verksamheten omfattas av säkerhetsskyddslagen, se 2 kap. 7 § säkerhetsskyddslagen (2018:585); Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 2; information som Riksrevisionen har tagit del av via mejl från företrädare för Länsstyrelsen Norrbotten, 2023-09-13; Länsstyrelsen Stockholm, 2023-07-07; Länsstyrelsen Västra Götaland, 2023-06-29; Länsstyrelsen Skåne, 2023-08-31.

223 2 kap. 12 § Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1).

säkerhetsskyddsåtgärder.[224] Säkerhetspolisen tillhandahåller vägledning i säkerhetsskydd som stöd i arbetet.[225] Enligt länsstyrelserna ses säkerhetsskydd på vissa håll som en fråga man helst inte vill vidröra vid lärosätena. Det beror dels på att det potentiellt kan försvåra ens dagliga verksamhet eftersom det kräver särskilda säkerhetsskyddsåtgärder, dels på att det kan vara känsligt i en verksamhet som vanligtvis präglas av öppenhet och internationalisering.[226] Lärosäten har även uttryckt att det behövs mer stöd för att göra bedömningar om antagonister och externa hot.[227]

Säkerhetspolisen anger att de håller föreläsningar om hot för i första hand lärosätenas säkerhetschefer, men sällan för fakultetsrepresentanter. Länsstyrelserna (Norrbotten, Skåne, Stockholm och Västra Götaland) ansvarar sedan december 2021 för tillsynen av säkerhetsskyddet, och kontakterna med lärosätena beskrivs hittills som begränsade. Några länsstyrelser beskriver att vissa lärosäten har varit svåra att få tag på. Hittills har ingen tillsyn initierats på något lärosäte.[228] Däremot kartlägger länsstyrelserna om lärosätena bedriver säkerhetskänslig verksamhet i enlighet med deras kartläggningsuppdrag som tillsynsmyndighet.[229]

---

224 Säkerhetsskyddslagen (2018:585); säkerhetsskyddsförordningen (2021:955); Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1). Riksrevisionen noterar att 11 lärosäten finns upptagna i säkerhetsskyddförordningens bilaga om myndigheter som beslutar om säkerhetsklass 2 och 3. Det finns dessutom lärosäten som angivit i Riksrevisioners enkät om informationssäkerhet del 2 att de bedriver säkerhetskänslig verksamhet, men som inte är upptagna i bilagan. Ytterligare ett lärosäte, som ej är med i vår granskning, har anmält till sin tillsynsmyndighet men är inte upptagna i förordningens bilaga. Regeringen har fattat beslut om att se över och föreslå förändringar av processen för säkerhetsprövningar, se dir. 2023:91 som ska redovisas senast 2024-08-15. Syftet är bl.a. att ge verksamhetsutövare tydliga förutsättningar för sitt säkerhetsskyddsarbete.

225 Se t.ex. Säkerhetspolisen, ”Vägledningar säkerhetsskydd”, hämtad 2023-10-30.

226 Intervju med företrädare för Länsstyrelsen Norrbotten, Länsstyrelsen Stockholm, Länsstyrelsen Västra Götaland och Länsstyrelsen Skåne, 2023-06-21.

227 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1; intervju KTH4.

228 Alla länsstyrelser med tillsynsuppdrag har inte lärosäten som har anmält att de bedriver säkerhetskänslig verksamhet, se mejl från företrädare för Länsstyrelsen Norrbotten, 2023-09-13; Länsstyrelsen Stockholm, 2023-07-07; Länsstyrelsen Västra Götaland, 2023-06-29; Länsstyrelsen Skåne, 2023-08-31.

229 Intervju med företrädare för Länsstyrelsen Norrbotten, Länsstyrelsen Stockholm, Länsstyrelsen Västra Götaland och Länsstyrelsen Skåne, 2023-06-21. Se också 8 kap. 4 § säkerhetsskyddsförordningen (2021:955).

4.4.3 Lärosätena har bristande kunskap om produkter med dubbla användningsområden och exportkontroll

Produkter med dubbla användningsområden (PDA) är produkter som kan användas både civilt och militärt. Vid export av PDA ut ur EU krävs alltid tillstånd. Granskningen visar på bristande rutiner för och kunskap om PDA och exportkontroll på lärosätena. Som en konsekvens läggs stort ansvar ofta på enskilda forskare och prefekter vilket ställer höga krav på att det finns tillräcklig kompetens bland berörda.

10 av 24 lärosätena uppger i sitt enkätsvar att de har en policy eller riktlinjer för exportkontroll.[230] Forskare uppger i intervjuer att det kan vara svårt att avgöra om ens forskningsdata kan komma att falla under regelverk för exportkontroll.[231] Vid KTH anger stödfunktionen för exportkontroll att fokus ligger på att hitta riskaktiviteter, exempelvis genom att vid förfrågan från forskare påtala riskerna med en viss finansiering i kombination med ett visst universitet och ämne.[232]

Myndigheten Inspektionen för strategiska produkter (ISP) inledde en särskild tillsyn mot universitet och högskolor 2018. Tillsynen beskrivs av både ISP och lärosäten som ett startskott för att arbeta mer strukturerat med frågor om PDA och exportkontroll.[233] ISP gjorde bedömningen att den svenska forskningssektorn bedriver framstående forskning inom känsliga forskningsområden som omfattas av exportkontroll, och sannolikt exporterar och överför exportkontrollerade produkter. Det innebär en reell risk för att känsliga exportkontrollerade produkter sprids för användning som går emot svensk utrikes- och säkerhetspolitik, såsom inom program for att utveckla massförstörelsevapen eller militär slutanvändning hos känsliga aktörer.[234]

---

230 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

231 Intervjuer KTH6; KTH16; LU9; LU26. Några exempel på sådana områden är artificiell intelligens, additiv tillverkning, nanovetenskap och informations- och kommunikationsteknologi. Exempel på PDA är olika slags material, kemikalier eller verktyg. Det är mindre vanligt att forskningsdata omfattas, men exempelvis källkoder samt data om grödor respektive djuphavsområden som samlas in av bildkamerasensorer och forskningsundervattenfarkoster kan utlösa exportkontroller för produkter med dubbla användningsområden. Vidare kräver en publikation exporttillstånd om den innehåller teknik som ska kontrolleras för dubbla användningsområden. Det gäller även eventuellt underlag i form av rådata, se ISP, ”Introduktion till produkter med dubbla användningsområden”, hämtad 2023-08-16. Se också Kommissionens rekommendation (EU) 2021/1700 av den 15 september 2021, avsnitt 2.2, tillägg 1 och tillägg 2.

232 Intervju KTH3.

233 Intervju med företrädare för ISP, 2022-09-16; intervjuer BTH6; KTH3; LU9.

234 ISP, *Projektrapport – universitetsprojektet,* 2022-12-29, s. 3–4.

ISP beskriver att okunskap och oklarheter rörande vilka produkter som är klassificerade fortfarande är utmaningar för lärosätena, liksom lärosätenas ofta decentraliserade struktur och en ovana att förhålla sig till externa regelverk som kan uppfattas inskränka den akademiska friheten. Det är också en utmaning att i ett tidigt stadium i forskningsprocessen kunna peka ut känsliga samarbeten.[235] En försvårande omständighet vid bedömning i exportkontrollärenden är dessutom att en falsk slutanvändare ibland uppges, vilket är svårt för lärosätena att kontrollera.[236]

4.4.4 Lärosätena har svårt att bedöma vad som avses med bakgrundskontroller i MSB:s föreskrifter

Granskningen visar att lärosätena tycker att det är oklart vilka bakgrundskontroller som avses i MSB:s föreskrifter, utöver vanlig referenstagning inför anställning. Oklarheter kan leda till att bakgrundskontrollerna som görs inte uppfyller sitt syfte. Olika tolkningar av samma regelverk inom och mellan lärosäten kan också leda till att åtkomsten till skyddsvärda data inte hanteras likvärdigt.

Av MSB:s föreskrifter om informationssäkerhet för statliga myndigheter framgår att bakgrundskontroller är en av flera säkerhetsåtgärder avseende behandling av information för att säkerställa att personal behandlar information på ett säkert sätt. Myndigheten ska därför ”anpassa bakgrundskontroller av egen och inhyrd personal utifrån vilken information personalen ska få åtkomst till”. Enligt allmänna råd bör bakgrundskontroller ske ”genom intervju, kontakt med referenser samt verifiering av akademiska, yrkesmässiga och övriga kvalifikationer”.[237] I bakgrundskontroller inkluderas inte den typ av säkerhetsprövning som görs inom ramen för säkerhetsskyddslagen även om det finns visst överlapp. För både säkerhetsprövning och bakgrundskontroll är syftet att den som anställer ska få en uppfattning om huruvida personen är pålitlig samt vilket behov som finns av utbildning i informationssäkerhet (eller säkerhetsskydd) för att personen i fråga ska kunna utföra sina arbetsuppgifter korrekt.[238]

Lärosätenas bakgrundskontroller tar sikte på akademiska meriter i samband med nyanställningar och rekrytering av doktorander. Det kan även ske intervjuer på

---

235 Intervju med företrädare för ISP, 2022-09-16; ISP, *Projektrapport – universitetsprojektet*, 2022-12-29, s. 12–17.

236 Intervju med företrädare för Säkerhetspolisen, 2022-10-20.

237 9 § 1 MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) jämte tillhörande allmänna råd.

238 Mejl från företrädare för MSB, 2023-09-14. En säkerhetsprövning enligt 3 kap. 2 § säkerhetsskyddslagen (2018:585) syftar även till att klarlägga om en person kan antas vara lojal mot de intressen som skyddas i säkerhetsskyddslagen,

initiativ av verksamheten när man bedömer att personen kan komma i kontakt med information som är skyddsvärd, uppger en intervjuad vid LU. På ledningsnivå vid LU har man börjat diskutera om de kontroller man hittills gjort kan behöva utökas, men menar att man inte har kompetensen att göra ytterligare bakgrundskontroller och efterlyser kompetens på central lärosätesnivå.[239]

4.4.5 Lärosätena efterlyser stöd vid riskbedömningar i internationella samarbeten

Både forskningsledare och prefekter i vår granskning påtalar behov av tydlig vägledning från såväl lärosätet som regering och ansvariga myndigheter när det gäller vissa internationella samarbeten.[240] Frågan har blivit högaktuell i och med de senaste årens säkerhetspolitiska utveckling.

BTH, KTH och LU har en hög grad av internationalisering i sina verksamheter.[241] Ett exempel på när mer stöd efterfrågas är det kinesiska stipendieprogrammet *China Scholarship Council* (CSC), som var aktuellt under tiden för våra intervjuer. Lärosätena som tog emot doktorander från CSC-programmet gjorde olika bedömningar av huruvida de skulle fortsätta, säga upp eller pausa samarbetet efter medias avslöjande om etiska tveksamheter i programmet i januari 2023.[242]
I Sveriges Kinastrategi lyfts utmaningarna i forsknings- och utbildningssamarbete rörande etik, akademisk frihet, immaterialrättsskydd samt kopplingar till den militära sektorn i Kina. Samtidigt framgår att ansvaret att hantera utmaningarna ligger på lärosätena och det forskningsintensiva näringslivet.[243]

Vi har i granskningen iakttagit exempel på att lärosäten själva tar initiativ till riktlinjer och checklistor som stöd vid internationella samarbeten.[244] Ett pågående regeringsuppdrag syftar också till att stötta lärosätena att göra bedömningar av internationella utbildnings- och forskningssamarbeten, se avsnitt 2.5.[245]

---

239 Intervjuer BTH2; BTH8; KTH11; LU1; LU6; LU9; LU14; LU21.

240 Intervjuer KTH6; KTH8; KTH9; KTH11; KTH14; LU4; LU14.

241 Exempelvis är mer än hälften av doktoranderna utländska vid BTH och KTH, se Stiftelsen för internationalisering av högre utbildning och forskning (STINT), ”STINT internationaliseringsindex”, hämtad 2023-09-18.

242 Nilsson, ”Kinas hemliga avtal med studenter i Sverige – kräver lojalitet med regimen”, 2023-01-12; intervjuer BTH10; KTH3; LU27.

243 Skr. 2019/20:18, s. 18.

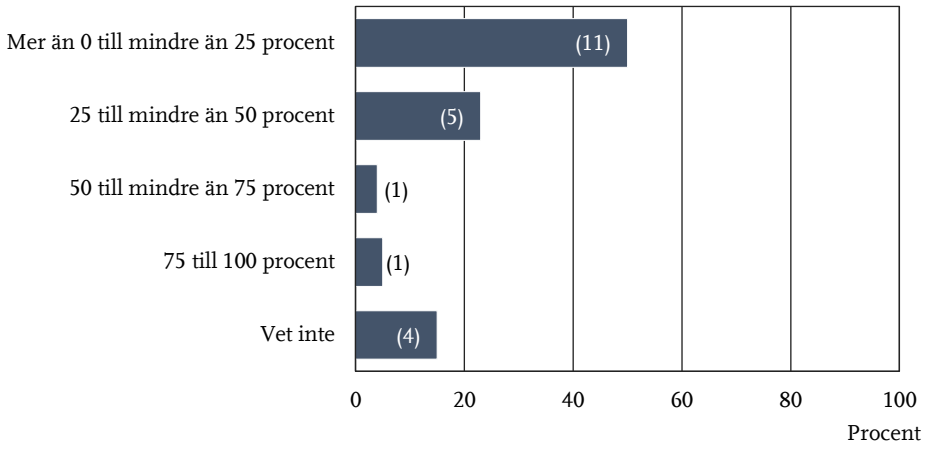
244 Stiftelsen för internationalisering av högre utbildning och forskning, *Responsible internationalisation: Guidelines for reflection on international academic collaboration*, R20:01; Lunds universitet, Sektionen Externa relationer, *Checklista för Globalt ansvarsfullt engagemang*, mars 2023; intervju LU27; mejl från rektor LTH, 2023-09-14.

245 Regeringsbeslut U2023/02127.

4.4.6 Lärosätenas utbildningar i informationssäkerhet får inte tillräckligt genomslag i forskningsverksamheten

Trots att ökad kunskap hos anställda har varit en av lärosätenas prioriteringar de senaste två åren har få medarbetare gått de utbildningar som ges.[246] Många universitet och högskolor konstaterar att det fortfarande finns stora behov av kompetenshöjning i informationssäkerhet.[247] 23 av 24 lärosäten erbjuder sina medarbetare utbildning i informationssäkerhet i form av fysiska eller digitala utbildningar. Som framgår av figur 5 nedan anger hälften av lärosätena att färre än 25 procent av medarbetarna har gått utbildningarna. Nästan tre fjärdedelar av lärosätena anger att färre än 50 procent har gjort det.[248]

Figur 5 Andel av lärosätets medarbetare som gått utbildning i informationssäkerhet



Källa: Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.
Anm.: Antal lärosäten inom parentes.

En utmaning för lärosätena är att den kompetens som byggs inom informationssäkerhet bland prefekter och dekaner kontinuerligt försvinner. Chief Information Security Officer vid LU beskriver det som att alla chefer därför måste

246 Även införandet av ledningssystem för informationssäkerhet samt inventering, klassning och analys har varit prioriterat, se Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1. De utbildningar som avses här är alltså de som är specifikt riktade till medarbetare vid lärosätena. För en beskrivning av andra typer av kompetenshöjande insatser inom området, se t.ex. Riksrevisionen, *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig*, RiR 2023:8, 2023, s. 39.

247 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1; intervjuer BTH2; BTH5; KTH4; KTH5; KTH6; KTH15; LU3; LU5; LU7; LU20.

248 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

"läras om från början" vart tredje eller fjärde år.[249] Riksrevisionen konstaterar att kontinuiteten därmed riskerar att gå förlorad, vilket kan påverka hur framgångsrikt informationssäkerhetsarbetet kan bedrivas.

75 procent av lärosätena uppger att de erbjuder utbildning i personuppgiftshantering och ungefär hälften erbjuder utbildningar i exempelvis forskningsdatahantering, forskningsetik och sekretess.[250] Utbildningarna som tillhandahålls är sällan obligatoriska. Vid LU erbjuds riktade utbildningar om datahanteringsplaner till nystartade forskningsprojekt men dessa är inte ett krav, även om projekten aktivt söks upp av ansvariga för forskningsdatahantering vid fakultetsbiblioteken.[251] Även vid KTH görs riktade utskick från biblioteket till forskare som beviljats anslag från externa finansiärer som kräver datahanteringsplaner.[252]

Det förekommer sällan någon systematisk uppföljning eller krav på att medarbetare ska uppdatera eller bibehålla sin kunskap i informationssäkerhet. Riksrevisionen har inte heller iakttagit att det sker någon systematisk uppföljning rörande medarbetares deltagande i informationssäkerhetsutbildningar.[253]

4.4.7 Lärosätena har initierat flera nätverk och samarbetsgrupper kring säkerhet och informationssäkerhet först på senare år

Riksrevisionen konstaterar att det är först på senare år som lärosätena har tagit initiativ till ökat samarbete inom säkerhets- och informationssäkerhetsområdet. Ett nätverk för säkerhet vid svenska lärosäten bildades 2020.[254] Samma år tog Sveriges universitets- och högskoleförbund (SUHF) initiativ till en säkerhetsutbildning i samarbete med Försvarshögskolan och Säkerhetspolisen. Det skedde efter uppmaningen från dåvarande ministern för högre utbildning och forskning att bedriva ett systematiskt säkerhetsarbete.[255] Utbildningen i säkerhets- och verksamhetsanalys fick dock ställas in på grund av bristande intresse. En förklaring till det låga intresset uppges vara att utbildningen vände sig till säkerhetsskyddschefer, vilket många lärosäten inte har. Under 2022 kom flera

249 Intervju LU2.

250 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

251 Intervju LU1.

252 Intervju KTH2.

253 Intervjuer BTH1; BTH11; BTH13; BTH15; KTH15; KTH16; LU3; LU7; LU17; LU19.

254 Skarsgård, "Nätverk ska förebygga spionage mot lärosäten", 2020-02-06; Eliasson, "Ökade hot mot lärosätena: 'Behov att växla upp säkerheten'", 2021-10-06.

255 SUHF, "Information från SUHF angående säkerhetsutbildning i sektorn", mejl till universitet och högskolor, 2020-05-07.

förfrågningar från lärosäten om nya kurstillfällen, men ingen ny utbildning riktad till högskolesektorn planeras. Försvarshögskolan har hänvisat till ordinarie kursverksamhet, men lärosätena har inte varit prioriterade och ofta inte fått plats.[256]

I oktober 2022 bildade SUHF en arbetsgrupp för informationssäkerhet inklusive it-/cybersäkerhet som en undergrupp till Expertgruppen för fastighets- och säkerhetsfrågor. Gruppen ska identifiera och föreslå åtgärder på informationssäkerhetsområdet, bland annat om strategier, handlingsplaner och regelverk inom sektorn, säker molnlagring samt samarbete kring klassning av informationstillgångar och risk- och sårbarhetsanalyser.[257] I oktober 2023 var gruppen i färd med bland annat att bilda ett nätverk för dem som arbetar med informationssäkerhet på lärosätena.[258]

4.5 Lärosätenas stöd för säker forskningsdatahantering är inte tillräckligt ändamålsenligt

Granskningen visar att det finns ett omfattande administrativt stöd för datahantering på olika organisatoriska nivåer, men forskare vet inte alltid vart de ska vända sig för att få stöd. Bristen på samordning mellan stöd för informationssäkerhet och stöd för tillgängliggörande av forskningsdata är ibland ineffektiv. Det finns också brister i det it-stöd som lärosätena erbjuder på central lärosätesnivå eftersom man inte kan tillhandhålla ytor för säker lagring och bevarande av stora mängder forskningsdata.

4.5.1 Stödet till forskare för säker datahantering har begränsat genomslag

Forskare och prefekter i vår granskning uppger att de inte alltid vet vem de ska vända sig till vid informationssäkerhetsfrågor som uppstår i det dagliga forskningsarbetet, exempelvis i fråga om forskningsdatabaser, datadelning med andra lärosäten och exportkontroll.[259]

---

256 Intervju med företrädare för Försvarshögskolan, 2022-06-27; mejl från företrädare för Försvarshögskolan 2023-10-11; intervju med företrädare för Stockholms universitet, 2022-08-25.

257 SUHF, ”Arbetsgruppen för informationssäkerhet och it-/cybersäkerhet”, hämtad 2023-10-04.

258 Mejl från företrädare för SUHF, 2023-10-11. Sedan tidigare finns också Sveriges universitet och högskolors it-chefsforum som syftar till erfarenhetsutbyte, samarbete och (digital) it-utveckling inom högskolesektorn. Forumet har ett antal nätverksgrupper, bl.a. drift och infrastruktur, it-säkerhet och it-forskningsstöd, se It-chefsforum, ”ITCF i korthet”, hämtad 2023-10-04.

259 Intervjuer BTH12; KTH12; KTH14; KTH17; LU17; LU18; LU19.

Många lärosäten arbetar med att skapa en enda ingång för forskningsrelaterade frågor på sina webbplatser för att underlätta för anställda.[260] Forskare som vi intervjuat i granskningen verkar dock föredra stöd i form av en personlig kontakt. Ofta associerar man stödfunktioner för informationssäkerhet specifikt till it-området.[261] I granskningen nämner både forskare och prefekter att de i första hand vänder sig till lokala it-samordnare på institutionerna vid LU[262] eller de administrativa cheferna på KTH:s skolor vid olika frågor som relaterar till informationssäkerhet. I granskningen nämndes också stödfunktioner vid förnamn eller refererades till som "it-killen" och "GDPR-ansvarig".[263]

Granskningen visar att det inte är tillräckligt att tillhandahålla skriftligt material om informationssäkerhet. Många forskare vet inte om att det finns eller läser det inte. Förståelse och efterlevnad av beslutade arbetssätt kan underlättas av att det finns tillgängliga medarbetare som man kan vända sig till för stöd. Ett exempel är just den utbredda kännedomen om dataskydd på grund av kravet på att utse dataskyddsombud.[264]

Flera av de vi intervjuat upplever att det kan saknas information om informationssäkerhet på engelska, vilket är ett problem för de många internationella forskare som finns på lärosätena.[265] I granskningen nämner också forskare att de söker stöd externt, eller stöd från mer seniora kollegor.[266] Vetenskapsrådet beskriver att man får frågor direkt från forskare om områden som

---

260 Se t.ex. KTH, "Forskningsstöd vid KTH", hämtad 2023-10-06; LU "Stöd till forskning vid LU", hämtad 2023-10-06; Malmö universitet, "Forskarstöd vid Malmö universitet", hämtad 2023-10-06. Informationssäkerhetsfrågor finns sällan med som en egen aspekt, men kan rymmas inom de delar som beskriver datahanteringsplaner.

261 Intervjuer KTH13; KTH15; LU16.

262 På sikt ska lokala informationssäkerhetssamordnare utses vid behov vid LU och fungera som kontaktpunkt gentemot CISO och lokala experter i operativa frågor, se Lunds universitet, Informationssäkerhetsbloggen, "Ledningssystem för informationssäkerhet har beslutats av rektor", hämtad 2023-09-06.

263 Intervjuer KTH1; KTH4; KTH9; KTH12, KTH11; LU17.

264 Samtliga 24 lärosäten har dataskyddsombud medan 12 har en informationssäkerhetschef, se Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

265 Intervjuer BTH15; KTH5; KTH11; KTH17; LU11; LU18; LU21. Det saknas också utbildningsmaterial på engelska på nationell nivå, exempelvis de webbutbildningar om informationssäkerhet som kan nås via MSB:s webbplats. MSB har dock påbörjat ett arbete med att tillhandahålla webbutbildningen DISA med engelsk text. Föreskrifterna för informationssäkerhet finns inte heller översatta eftersom MSB inte sett det behovet. Däremot finns vägledningen till stöd för arbetet hos statliga myndigheter med säkerhetsåtgärder i informationssystem (MSBFS 2020:7) översatt till engelska, se mejl från företrädare för MSB, 2023-11-07.

266 Intervjuer BTH6; BTH8; BTH12; KTH12; KTH18; LU19; LU29.

lärosätena själva ska ha kunskap om.[267] Det tyder på att det kan finnas behov av förtydliganden hos lärosätena. Risken med att ta hjälp av kollegor är att de ger stöd som inte är i enlighet med lärosätenas centrala riktlinjer och därmed kan felaktig eller bristfällig kunskap spridas i organisationen.

Riksrevisionen har också noterat att forskarna inte alltid sätter sig in i det administrativa stöd som erbjuds och att det kan uppfattas som kostsamt administrativt extraarbete. Som vi tidigare redogjort för finns det exempelvis forskare som tycker att datahanteringsplaner är onödiga. Forskare vi intervjuat vet i många fall om att det finns styrdokument om informationssäkerhet, men inte vad de innehåller eller hur de ska användas i praktiken.[268] Vid flera intervjuer letade intervjupersonerna vid sittande bord efter vägledningar på respektive lärosätes intranät och kunde konstatera att det fanns information de inte tagit del av tidigare. I några fall hade intervjupersonerna precis innan vår intervju blivit varse att det fanns ett omfattande stödmaterial, eller blivit informerade av vår kontaktperson på lärosätet om materialet.

4.5.2 Stödet i frågor som rör säker datahantering är inte alltid samordnat men det finns initiativ för ökad samverkan

Stödet inom informationssäkerhet respektive hanteringen av forskningsdata har traditionellt varit uppdelat mellan it och bibliotek vilket ställer krav på samordning. 22 av 24 lärosäten i granskningen anger att de har forskningsdatateam eller motsvarande, ofta kallade Data Access Units (DAU:er) som erbjuder stöd till forskare i frågor som rör bland annat tillgängliggörande och bevarande av forskningsdata. Forskningsdatateamen är normalt sett organiserade på biblioteken och kan finnas på olika nivåer i organisationen. Av Riksrevisionens enkät framgår att det oftast saknas någon person med särskild kompetens i informationssäkerhet i forskningsdatateamen. På motsvarande sätt saknar ofta informationssäkerhetsgrupper vid lärosätena särskild kompetens inom forskningsdatahantering.[269] Riksrevisionen konstaterar att bristande samordning kan vara ineffektivt och försvåra det dagliga arbetet för forskarna.

---

267 Det handlar exempelvis om vilka typer av data som får göras öppet tillgängliga och vad som gäller för upphovsrättsligt skydd av data samt frågor om datalagring. Intervju med företrädare för Vetenskapsrådet, 2023-05-24; mejl från företrädare för Vetenskapsrådet, 2023-09-13.

268 Intervjuer BTH1; BTH3; BTH5; BTH7; KTH2; KTH3; LU5; LU11; LU22; LU23. Se också bl.a. Ander, T., *Informationssäkerhetskultur*, 2022, s. 89 om vikten av att informationssäkerhetsarbetet inte uppfattas som ännu en pålaga av medarbetarna.

269 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

Granskningen visar att det vid KTH och LU finns initiativ för att få med informationssäkerhetsaspekten i stödet rörande forskningsdatahantering. LU har forskningsdatastöd på universitetsbiblioteket och på fakultetsbiblioteken. Forskningsdatastödet vid universitetsbiblioteket har kontakt med andra relevanta funktioner, inklusive Chief Information Security Officer.[270] Fakulteternas forskningsdatastöd jobbar mer forskarnära, exempelvis med att stötta forskare i upprättandet av datahanteringsplaner.[271]

Fakultetsbibliotekens forskningsdatastöd vid Naturvetenskapliga fakulteten och Lunds tekniska högskola uttrycker att de har behov av tillgång till ytterligare kompetens eftersom de ofta får frågor rörande it, arkivering och juridik som de inte kan besvara direkt. Forskningsdatastödet vid Naturvetenskapliga fakulteten vid LU har på eget initiativ skapat en arbetsgrupp som inkluderar funktioner från arkiv och it som träffas en gång i månaden. Stödet har också tagit fram en självstudiekurs om hur man upprättar en datahanteringsplan och låt funktionerna it och arkiv granska manus under framtagandet. När kursen var klar erbjöd man de andra fakultetsbiblioteken att använda den, men man vet inte om den faktiskt används.[272] Riksrevisionen konstaterar att det kan vara ineffektivt om den här typen av erfarenheter och kunskap inte delas i tillräcklig utsträckning.

KTH inrättade en grupp för forskningsdatastöd kring tillgängliggörande som ett internt utvecklingsprojekt 2019, som därefter permanentats. 2019 inrättades även en tjänst som forskningsdatakoordinator för att koordinera arbetet i gruppen som består av personal från bibliotek, forskarstöd och it-avdelning. 2021 kompletterades denna grupp med ytterligare en arbetsgrupp för forskningsdata med fokus på skydd av forskningsdata som består av forskningsdatakoordinator, it- och informationssäkerhetschef, informationssäkerhetsspecialist och dataskyddsombud. Denna grupp arbetar operativt med ärenden i samarbete med relevanta funktioner som jurister samt i mån av tid med att ta fram anvisningar för informationshanteringen i forskningsverksamheten.[273]

19 lärosäten uppger i enkäten att de har särskilda informationssäkerhetsgrupper. I dessa grupper ingår sällan personer med särskild kompetens inom forskningsdatahantering.[274] Mot bakgrund av våra iakttagelser ovan kan det finnas skäl att även inkludera funktioner inom forskningsdatahantering (vanligtvis

270 Intervjuer LU8; LU11; LU12.
271 Intervju LU11.
272 Intervjuer LU11; LU12.
273 Intervjuer KTH2; KTH, *Svar på den inkomna rapporten från Riksrevisionen*, 2023-10-26.
274 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

organiserade vid biblioteken) i dessa informationssäkerhetsgrupper. Det kan stärka samordningen mellan stödfunktionerna när det gäller forskningsdatahantering.

4.5.3 Lärosätena erbjuder inte säkra ytor för lagring och bevarande av forskningsdata

Inget lärosäte erbjuder kompletta tjänster för långsiktigt bevarande av forskningsdata och forskningsresultat. Lärosätena har också utmaningar att tillhandhålla lagring av stora datamängder under pågående forskningsprojekt. Följden blir ad hoc-lösningar beroende på vilka behov enskilda forskningsprojekt har.

Avsaknaden av säkra molntjänster för att hantera till exempel känsliga personuppgifter nämns som problematiskt av flera lärosäten.[275] Det finns också begränsningar när det gäller hur stora datamängder som kan lagras till en rimlig kostnad. Forskare beskriver hur stora datamängder därför förvaras på forskares egna servrar eller servrar och beräkningsdatorer på institutionen och säkerhetskopieras på externa hårddiskar som placeras på olika platser.[276]
Det förekommer också att riktigt stora datamängder har backup hos externa samarbetspartner som SciLifeLab eller Cern i Schweiz eftersom lärosätena inte kan tillhandahålla lagring i den storleksordningen.[277]

En annan konsekvens av avsaknaden av lärosätesgemensamma lagringslösningar är att enskilda forskningsprojekt själva får vara med och bekosta lagring av forskningsdata under pågående projekt. Resultatet blir att informationssäkerhet vägs mot forskarens kostnad för datalagring och i flera intervjuer har frågan kommit upp vem som ska betala för säkerheten när data lagras.[278] Det finns möjlighet att i forskningsansökningar ansöka om medel för att täcka kostnader för lagring av data. Beviljade ansökningar ger dock finansiering för tre till fyra år i normala fall, medan behoven av lagring ofta sträcker sig betydligt längre än så.[279]

LU är i färd med att införa en lösning på central lärosätesnivå för långtidslagring av forskningsdata. Det är dock oklart hur stora mängder data som kommer att kunna

---

275 Riksrevisionens enkät om informationssäkerhet till 24 lärosäten, del 1.

276 Intervjuer KTH18; KTH9; LU19; LU21.

277 Intervjuer KTH18; LU11.

278 Intervjuer KTH9; KTH18; LU12; LU13; LU18: LU19; LU20; LU21; LU25.

279 Gängse praxis på många lärosäten är en gallringsfrist på 10 år för forskningsdata och 15 år för medicinska forskningsdata. Det beror bl.a. på att forskningsinformation och forskningsdata ska sparas i minst 10 år för att kunna presenteras vid en prövning om oredlighet, se SUHF, 2022. Vissa forskningsdata ska aldrig gallras, se 6–7 §§ Riksarkivets föreskrifter och allmänna råd om gallring av handlingar i statliga myndigheters forskningsverksamhet (RA-FS 1999:1)

hanteras där. LU uppskattar att det läggs cirka en miljard kronor om året på it. Det finns en förhoppning om att mer centraliserade it-lösningar kommer att bidra till att kostnaderna reduceras. Flera prefekter vid LU framhåller att obligatoriska krav på forskarna från den centrala lärosätesledningen även bör medföra finansiellt stöd från centralt håll.[280]

På nationell nivå har Sveriges universitetsdatanätverk (Sunet) i uppgift att tillhandahålla datanät för landets universitet och högskolor. Sunet erbjuder också ett antal onlinetjänster för forskning och utbildning.[281] Sunet Drive är en tjänst som erbjuds av Sunet för att lagra och dela data. I november 2023 hade tjänsten 18 kunder, varav alla var lärosäten. Det pågår ett arbete för att göra det möjligt att koppla åtkomst till känsliga dokument mot förstärkt inloggning.[282] Sunet säger att de har outnyttjad kapacitet men att tjänsterna inte efterfrågas av lärosätena.[283]

I SUHF:s *Färdplan för öppen vetenskap* rekommenderas lärosätena att senast 2025 ”erbjuda forskare prisvärda, adekvata och säkra infrastrukturella tjänster – som uppfyller gällande regelverk (framför allt tryckfrihetsförordningen, offentlighet- och sekretesslagen, arkivlagen och GDPR) och FAIR-principerna – för hantering, lagring, tillgängliggörande och bevarande av forskningsdata och forskningsresultat där arkivering och gallring ingår som en integrerad del i forskningsprocessen och arbetet med öppen tillgång”.[284] I en enkät om arbetet med att implementera färdplanen framgår att 2 lärosäten under 2023 har ”en heltäckande och behovsanpassad uppsättning av e-infrastrukturtjänster, arbetsprocesser och arbetsflöden samt rådgivning kring god hantering av forskningsdata”. 25 lärosäten har påbörjat arbetet och 3 har inte påbörjat arbetet.[285]

280 Intervju LU3; LU4; LU16.

281 Sunet, ”Tjänster”, hämtad 2023-09-29. Utöver 40 universitet och högskolor är 16 myndigheter, 14 muséer, 3 forskningsinfrastrukturer och 18 övriga organisationer anslutna till Sunet, se Sunet, ”Anslutna organisationer”, hämtad 2023-11-12.

282 Mejl från företrädare för Sunet, 2023-11-12; Sunet, *Protokoll fört vid kommittésammanträdet 2023-06-01*.

283 Intervju med företrädare för Sunet, 2023-05-29.

284 SUHF, *Vägledning för implementering av färdplan för öppen vetenskap*, 2022-06-30, s. 8.

285 SUHF, *Vägledning med åtgärdsförslag för implementering av färdplan för öppen vetenskap. Sammanställning enkät 2023*. En förklaring till att lärosätena avvaktat med att ta itu med exempelvis hantering, lagring och arkivering av forskningsdata för övergången till ett system för öppen vetenskap kan vara att de statliga lärosätena inte har regleringar eller uppdrag från regeringen inom digitalisering av forskning eller digital infrastruktur för forskning, se SOU 2021:65, s. 206.

5 Slutsatser och rekommendationer

Riksrevisionens övergripande slutsats är universitet och högskolor inte bedriver ett effektivt informationssäkerhetsarbete för att skydda forskningsdata. Trots att föreskriftskrav funnits sedan 2008 och bristerna varit kända sedan länge saknas fortfarande väsentliga delar av ett systematiskt informationssäkerhetsarbete. De åtgärder som regering, lärosäten och andra berörda myndigheter hittills vidtagit har inte varit tillräckliga.

5.1 Lärosätena arbetar inte effektivt för att identifiera skyddsvärda forskningsdata

En övervägande del av forskningsdata behöver inte skyddas utan kan vara öppen och tillgänglig för alla. Men för att kunna identifiera vilka data som är skyddsvärda behövs kännedom om de forskningsdata som hanteras i verksamheterna. Riksrevisionen bedömer att lärosätena har otillräcklig kännedom om verksamheternas skyddsvärda forskningsdata, och om dessa data hanteras enligt sina skyddsbehov och gällande regelverk. Det beror bland annat på bristande systematik i inventering och klassning av forskningsdata. Det leder till otillräckliga underlag för såväl riskbedömning som införande av ändamålsenliga säkerhetsåtgärder.

5.1.1 Bristande systematik i hur lärosätena identifierar skyddsvärda forskningsdata

Få forskare klassar sina forskningsdata enligt lärosätenas beslutade modeller för informationsklassning. Bristande rutiner för inventering och klassning av forskningsdata riskerar att leda till att vissa skyddsvärda forskningsdata inte identifieras. Att det finns olika rutiner inom samma lärosäte kan också leda till olika bedömningar av vad som är skyddsvärt. Avsaknaden av informationsklassning enligt en lärosätesgemensam modell kan även innebära dubbelarbete och vara tidskrävande.

En konsekvens av att informationsklassningar inte genomförs systematiskt och dokumenteras är att lärosätena får ett bristfälligt underlag för införandet av säkerhetsåtgärder. Det kan till exempel göra det svårare att få en uppfattning om vilka tjänster – såsom ytor för datalagring – som forskare behöver för att kunna hantera sina data säkert. Vidare visar granskningen att avsaknaden av ändamålsenligt utformade it-tjänster och säkerhetsåtgärder bidrar till att forskare tar fram egna lösningar. Riksrevisionen bedömer att det kan få konsekvensen att

forskningsdata inte skyddas från obehöriga och att likvärdig information får olika skydd.

Trots bristerna sker viss inventering och värdering av forskningsdata genom diverse arbetsprocesser och av flera olika funktioner inom lärosätena. Det förekommer att hanteringen av forskningsdata regleras genom att finansiärer och externa samarbetspartner ställer krav på datahanteringsplaner där forskningsdata ska klassas. Dessa planer sammanställs dock normalt inte av lärosätena. Det är inte heller alla forskningsprojekt som berörs. Det är också vanligt att forskarna gör egna mindre formaliserade bedömningar av skyddsvärden och skyddsbehov som inte dokumenteras.

Riksrevisionen bedömer att bristerna till stor del beror på att lärosätena inte har prioriterat arbetet med att inventera och klassificera forskningsdata. Lärosätesledningarna har inte i tillräcklig omfattning infört ändamålsenliga lärosätesövergripande arbetssätt för att identifiera skyddsvärd information. De har inte sett till att det finns ett tillräckligt bra stöd till prefekter och forskare för att kunna genomföra arbetet. Den kollegiala styrningen och lärosätenas ofta decentraliserade organisationsstruktur skapar utmaningar i styrning och implementering av ett systematiskt informationssäkerhetsarbete. Den stora andelen extern forskningsfinansiering och de olika krav som följer kan också bidra till att förklara avsaknaden av lärosätegemensamma arbetssätt.

5.1.2 Informationssäkerhet för forskningsdata är inte integrerat i lärosätenas riskanalyser

För att kunna göra ändamålsenliga riskbedömningar som inkluderar forskningsdata måste dessa först ha klassats. Riksrevisionen konstaterar att det ofta saknas förutsättningar för att göra sådana bedömningar eftersom forskningsdata inte klassas systematiskt enligt de modeller som lärosätet beslutat om. Granskningen visar att riskbedömningar kring forskningsdata ofta saknas på lärosätesövergripande nivå. Det är också ovanligt att fakulteter och institutioner genomför och dokumenterar bedömningar av informationssäkerhetsrisker överlag. Det kan leda till att informationssäkerhetsrisker för forskningsdata inte identifieras, analyseras och hanteras. Riksrevisionen konstaterar även att informationssäkerhet för forskningsdata inte inkluderas i tillräckligt hög utsträckning i den dialog om risker som förs mellan institutioner, fakulteter och central lärosätesnivå.

Granskningen visar vidare att forskare ofta gör löpande riskbedömningar i sitt arbete som inte nödvändigtvis dokumenteras eller kommuniceras, eller dokumenteras i exempelvis en datahanteringsplan eller i avtal med extern samarbetspartner. En förutsättning för ett effektivt riskarbete som tar hänsyn till hela verksamheten, inklusive forskningsdata, är att institutionernas riskbedömningar samlas upp och kommuniceras vidare. Riksrevisionen bedömer att lärosätenas brister i riskhanteringen rörande forskningsdata kan innebära högre risknivåer än vad man är medveten om eller är villig att acceptera.

5.2 Lärosätena har otillräcklig kunskap och kompetens att bedöma vad som är skyddsvärt

Riksrevisionen bedömer att kunskap och kompetens i frågor kopplade till informationssäkerhet överlag är bristfälliga hos många medarbetare. Det gäller kunskap såväl om hur man praktiskt ska arbeta för att skydda sin information, som om att klassa sina forskningsdata och förhålla sig till gällande regelverk och externa krav. Utbildningsinsatser når bara en liten del av lärosätenas personal. Lärosätena följer generellt sett heller inte upp genomgången utbildning.

Det saknas samsyn och kunskap både inom och mellan lärosäten om vad som är skyddsvärt och vilka skyddsvärden som finns kopplade till olika regelverk, exempelvis säkerhetsskyddslagen (2018:585). Bedömningen av skyddsvärden och skyddsbehov kräver inte bara förståelse för forskningen och dess värde, utan även kunskap om interna och externa intressenter, antagonister, hotbilder och juridiska krav.

Det räcker dessutom inte alltid att forskare har kännedom om skyddsvärden och risker kopplade till sina egna forskningsdata. Vissa risker uppstår först när data aggregeras, till exempel om en obehörig får tillgång till forskningsdata från olika verksamheter. Utan kunskap om vilka forskningsdata som är skyddsvärda på grund av exempelvis nationell säkerhet eller personlig integritet kan inte säkerhetsåtgärder dimensioneras på ett ändamålsenligt sätt.

Riksrevisionens granskning visar att medarbetare med dessa kompetenser, som till exempel informationssäkerhetschefer, säkerhetschefer och jurister, inte samverkar i tillräcklig utsträckning med forskarna för att bedöma risker relaterade till skyddsvärd information. Det är i sammanhanget en utmaning att dekaner och prefekter byts ut regelbundet eftersom det påverkar kontinuiteten i den kompetens som byggs upp i organisationen. För att upprätthålla kontinuiteten behöver det därför finnas rutiner och arbetssätt som inte är personberoende.

5.3 Lärosätesledningarna har inte styrt och organiserat informationssäkerhetsarbetet på ett effektivt sätt

I granskningen har Riksrevisionen sett exempel på otydligt ansvar, oklara delegationer och otydliga mandat. Det förekommer att lärosätena har informationssäkerhetspolicyer och delegationsordningar som inte är uppdaterade och som anger roller som inte finns i praktiken. Riksrevisionen konstaterar att även om ansvar för informationssäkerhet kan framgå av riktlinjer eller motsvarande kan det vara svårt för medarbetare att veta vad det innebär rent praktiskt.

Granskningen visar att nästan hälften av lärosätena har placerat den som är ansvarig för att samordna informationssäkerhetsarbetet på it-avdelningen. Det kan vara en konsekvens av att informationssäkerhetsarbetet av tradition har bedrivits med fokus på it-säkerhet. Riksrevisionen bedömer att placeringen kan utgöra ett hinder för att arbeta strategiskt på lärosätesövergripande nivå. Dessutom försvåras möjligheten att verka oberoende och kravställande i förhållande till it-organisationen. Den informationssäkerhetsansvariga rapporterar inte alltid heller regelbundet till styrelse eller rektor.

Prefekterna innehar en nyckelroll som verksamhetsansvariga på institutionerna. Det är ofta via prefekterna som forskarnas behov av informationssäkerhetsåtgärder kan fångas upp och föras vidare. Men granskningen visar att såväl prefekter som forskare på institutioner vid samma lärosäte har olika uppfattning om sitt ansvar. Otydligheter om vem som är informationsägare och vad det ansvaret innebär leder till oklarheter i fråga om vem som ytterst ansvarar för att ändamålsenliga säkerhetsåtgärder införs och att forskningsdata skyddas i enlighet med gällande regelverk.

Att forskare inte vet vart de ska vända sig för stöd när det gäller hantering av forskningsdata kan bero på att stödet inte är lättillgängligt och verksamhetsanpassat. Men det kan också bero på att forskarna inte har förstått att det finns beslutade arbetssätt som alla förväntas jobba utefter. Riksrevisionens bedömning är att lärosätesledningarna inte gjort tillräckligt för att se till att beslutade riktlinjer implementeras i hela organisationen.

Riksrevisionen har inte gjort en bedömning av huruvida avsatta resurser för informationssäkerhet är tillräckliga men konstaterar att de varierar stort mellan lärosätena. En förklaring till det kan förstås vara skillnader i lärosätenas storlek och inriktning. Det är dock få lärosäten som kan ange hur mycket resurser som avsätts för informationssäkerhet på central lärosätesnivå, bland annat därför att arbetet är utspritt på många funktioner. Flera lärosäten uppger att de har svårt att rekrytera

och behålla den kompetens de behöver för att kunna bedriva ett systematiskt informationssäkerhetsarbete.

Riksrevisionen har iakttagit att flera lärosäten brottas med liknande utmaningar när det gäller frågor om informationssäkerhet. Det gäller framför allt behovet av att höja den allmänna kunskapsnivån i informationssäkerhet bland forskande och undervisande personal, att kunna erbjuda tekniska lösningar för överföring, bearbetning och lagring av forskningsdata, samt utmaningen i att navigera i olika regelverk kring forskningsdata. Lärosätena har genom Sveriges universitets- och högskoleförbund (SUHF) tagit vissa initiativ till kompetenshöjning i sektorn, exempelvis genom samarbete med Försvarshögskolan och bildandet av särskilda expert- och arbetsgrupper inom informationssäkerhet och säkerhet. På enskilda lärosäten förekommer också kompetenshöjande aktiviteter och organisationsförändringar i syfte att förbättra informationssäkerhetsarbetet. Riksrevisionen ser positivt på dessa initiativ men bedömer att de har kommit för sent och varit otillräckliga. Sammantaget bedömer Riksrevisionen att lärosätesledningarna inte gett arbetet med informationssäkerhet tillräcklig prioritet.

5.4 Regeringens och myndigheternas åtgärder för att stärka informationssäkerhetsarbetet vid lärosätena har varit otillräckliga

Riksrevisionen konstaterar att regeringen varit senfärdig i sin uppföljning av informationssäkerheten vid lärosätena, trots att kunskap funnits om att den är bristfällig. Säkerhetsfrågor började tas upp i Regeringskansliets myndighetsdialoger med lärosätena först 2019. Regeringen har beslutat om flera uppdrag till lärosätena i form av bland annat återrapporteringskrav om informationssäkerhet 2022 och 2023. Det är för tidigt att uttala sig om effekterna av dessa uppdrag.

Regeringen har även gett uppdrag till MSB som en del av sin övergripande styrning av informationssäkerheten vid myndigheter. Riksrevisionen bedömer att dessa uppdrag och åtgärder varit otillräckliga för att stärka informationssäkerheten vid lärosätena. Genom verktyget Infosäkkollen, som MSB utvecklat, finns en begränsad möjlighet för regeringen att återkommande följa upp det systematiska informationssäkerhetsarbetet i offentlig sektor. Det beror bland annat på att Infosäkkollen är frivillig och i första hand framtagen för att organisationerna själva ska kunna utveckla sitt informationssäkerhetsarbete. I Infosäkkollen 2021 medverkade dessutom bara 15 lärosäten.

Sedan slutet av 2022 erbjuder MSB en rådgivningstjänst där myndigheter kan boka individuell rådgivning, utöver att skicka in frågor. De frågor som kommer in från lärosätena visar bland annat att förståelsen för informationssäkerhetschefens strategiska roll brister. Riksrevisionen bedömer att det är bra att Infosäkkollen och rådgivningstjänsten finns men att de inte utnyttjas i tillräckligt hög utsträckning som kompetenshöjande och rådgivande verktyg för lärosätena.

MSB har inte riktat några särskilda insatser till universitets- och högskolesektorn. Granskningen visar att lärosätena har särskilda förutsättningar exempelvis i fråga om stora och diversifierade datamängder med krav på öppenhet och tillgängliggörande. De är också decentraliserade organisationer med inslag av kollegial styrning där akademiska chefer regelbundet byts ut. Samtidigt är det tydligt i såväl MSB:s föreskrifter som MSB:s metodstöd att utformningen av informationssäkerhetsarbetet ska anpassas efter respektive verksamhets aktuella behov.

Myndigheter som Säkerhetspolisen och Inspektionen för strategiska produkter har genomfört vissa utbildningsinsatser vid lärosätena, men dessa har inte fått tillräckligt genomslag. Sedan december 2021 har de fyra länsstyrelserna Norrbotten, Skåne, Stockholm och Västra Götaland tillsynsansvar för säkerhetsskydd för lärosätena men ingen tillsyn har hittills genomförts.

5.5 Rekommendationer

Riksrevisionen bedömer att informationssäkerhetsarbetet vid universitet och högskolor gällande forskningsdata under lång tid överlag har varit eftersatt. Riksrevisionen lämnar därför nedanstående rekommendationer till regeringen och universitet och högskolor i syfte att snabbt få ett systematiskt informationssäkerhetsarbete på plats.

Till regeringen

- Ge uppdrag till Myndigheten för samhällsskydd och beredskap att genomföra kompetenshöjande insatser till ledningarna för universitet och högskolor. Insatserna bör anpassas efter lärosätenas behov.
- Ge uppdrag till universitet och högskolor att i samverkan inrätta en gemensam stödfunktion för informationssäkerhet. Etableringen bör ske i samråd med Myndigheten för samhällsskydd och beredskap och andra relevanta myndigheter. Dessa myndigheter bör även ge råd och stöd efter att funktionen etablerats. Stödfunktionen ska kunna bistå universitet och högskolor med bland annat följande:

- rådgivning till dem som leder och samordnar informationssäkerhetsarbetet om bland annat utformning av informationssäkerhetsarbetet, analys, säkerhetsåtgärder samt tolkning och efterlevnad av regelverk om till exempel säkerhetsskydd och exportkontroll
- behovsanpassade utbildningar och kurser i informationssäkerhet för samtliga medarbetare vid lärosätena
- stöd för att analysera och bedöma sektorsgemensamma risker och externa hot till relevanta funktioner på lärosätena.

Stödfunktionen kan med fördel dra nytta av kunskap och erfarenheter från bland annat pågående lärosätesgemensamma samarbeten och nätverk inom informationssäkerhetsområdet.

Till de 24 universitet och högskolor som ingår i granskningen

- Se till att roller och ansvarsfördelning är tydliga från ledningsnivå till enskilda medarbetare, så att varje medarbetare vet sitt ansvar när det gäller att hantera forskningsdata korrekt.
- Se till att de som leder det strategiska informationssäkerhetsarbetet har mandat att ställa krav och granska informationssäkerhetsarbetet samt att de regelbundet rapporterar till lärosätesledning och styrelse.
- Se till att arbetssätten för informationsklassning av forskningsdata är enhetliga.
- Se till att det finns kompetens att analysera informationssäkerhetsrisker kopplade till forskningsdata.
- Se till att det finns ett samordnat stöd för medarbetare att hantera forskningsdata korrekt under hela livscykeln.

Ordlista[286]

Chief Information Security Officer (CISO)
Roll med ansvar för att leda och samordna arbetet med informationssäkerhet i en organisation. CISO är informationssäkerhetssamordnare på högsta organisatoriska nivå. Se också avsnitt 2.4, Roller och funktioner på lärosäten.

Forskningsdata
Forskningsdata avser data som samlas in eller framställs inom ramen för vetenskaplig forskningsverksamhet. Det kan till exempel vara digitala texter, bilder, audiovisuella material, 3D-skanningar, observationsdata, resultat från experiment och andra typer av digitala objekt.[287] Statliga universitet och högskolor ansvarar för arkivbildning av sina allmänna handlingar. Här ingår forskningsinformation och forskningsdata.[288]

Forskningsämnesområde
Den högsta nivån i standarden för svensk indelning i forskningsämnen omfattar sex forskningsämnesområden: naturvetenskap, teknik, medicin och hälsovetenskap, lantbruksvetenskap och veterinärmedicin, samhällsvetenskap samt humaniora och konst. Under vart och ett av dessa sex forskningsämnesområden finns det på nästa nivå fem till elva forskningsämnesgrupper.[289]

Informationsklassning
Att klassa sin information avseende konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få.[290]

Informationsmängd
En gruppering av information, exempelvis i form av dokument, en databas eller liknande, som innehåller flera informationstyper.

Informationssäkerhet
Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.[291] Informationssäkerhet innefattar både organisatorisk säkerhet och teknisk säkerhet (se vidare Säkerhetsåtgärder).

---

286 Alla definitioner är från MSB, ”Termbanken för informationssäkerhet”, om inte annat anges.
287 Vetenskapsrådet, *Indikatorer för öppen tillgång till forskningsdata*, 1 mars 2023, s. 4.
288 SUHF, *Rekommendation om tillämpning av regelverk angående gallring och bevarande av forskningsinformation*. Antagen av SUHF:s styrelse 2022-04-26.
289 SCB, ”Standard för svensk indelning av forskningsämnen”, hämtad 2022-11-09.
290 6 § 1 MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).
291 3 § MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

Informationssäkerhetsincident
Enskild eller flera oönskade eller oväntade informationssäkerhetshändelser som har negativa konsekvenser för verksamheten och dess informationssäkerhet. Informationssäkerhetsincidenter kan samtidigt vara andra typer av incidenter såsom personuppgiftsincidenter.

Informationssäkerhetskultur
Gemensamma tanke-, beteende- och värderingsmönster som uppstår och utvecklas i ett socialt kollektiv genom kommunikativa processer, baserade på inre och yttre krav. Informationssäkerhetskulturen överförs till nya medlemmar och kan vara såväl bra som dålig eftersom begreppet inte är normativt.[292]

Informationstillgång
Information och informationsbehandlande resurser som är av värde för en organisation.

Informationstyp
En informationstyp är ett visst slag av information. En informationstyp kan finnas lokalt i en verksamhet eller vara spridd över hela organisationen, som exempelvis personuppgifter.[293]

Informationsägare
Befattningar som är ansvariga för att säkerställa att information skyddas på avsett sätt.[294]

Kollegialitet
Kollegialitet lägger stor vikt vid att ta tillvara medarbetarnas kunskap, erfarenhet och yrkesetik. Kollegialitet brukar därför förknippas med begreppet profession och är inte unikt för akademin. I en renodlad kollegial organisation inom akademin är kollegialt beslutsfattande och kollegiala ledarval (att kollegorna väljer sina ledare) viktiga grundprinciper, och de som inkluderas i kollegiet är de vetenskapligt kompetenta.[295]

Konfidentialitet
Konfidentialitet är egenskap hos informationstillgång som innebär att den inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer.

---

292 Hallberg m.fl., *Informationssäkerhet och organisationskultur*, 2017, s. 19–20.
293 MSB, ”Vägledning, Klassning av information”, hämtad 2023-10-30.
294 5 § MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) jämte tillhörande allmänna råd.
295 SOU 2015:92, s. 127 ff.

Ledningssystem för informationssäkerhet
Del av myndighetens övergripande ledningssystem, baserat på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och utveckla organisationens informationssäkerhet.[296]
Ledningssystemet omfattar organisationsstruktur, policyer, planeringsaktiviteter, ansvar, praxis, rutiner, processer och resurser.

Livscykelbedömning
Informationens värde och riskerna kan variera under hela informationens livscykel, från det att informationen skapas till att den gallras (eller långsiktigt bevaras). Informationssäkerheten blir därför i viss utsträckning viktig i alla stadier.[297]

Riktighet
Egenskap hos informationstillgång som innebär att den skyddas mot oönskad förändring.

Riskanalys
Process för att förstå riskens natur och för att avgöra risknivån.

Riskbedömning
Övergripande process som innefattar delprocesserna riskidentifiering, riskanalys och riskutvärdering.

Skyddsvärda data
Med skyddsvärda forskningsdata avses i den här granskningen i första hand sådana data som behöver skyddas på grund av sekretess eller dataskyddsreglering eller annan specialreglering. Det kan exempelvis röra stora mängder eller känsliga personuppgifter, företagshemligheter eller säkerhetskänslig verksamhet.[298]

Spårbarhet
Entydig härledning av utförda aktiviteter till en identifierad användare.

296 3 § MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).
297 Svenska institutet för standarder, *Svensk standard SS-ISO/IEC 27002:2022, Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder* (ISO/IEC 27002:2022, IDT), utgåva 3, s. viii.
298 Riksrevisionens definition, se även avsnitt 1.1.

Säkerhetskänslig verksamhet
Säkerhetskänslig verksamhet är sådan verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd. Uttrycket Sveriges säkerhet tar sikte på sådant som är av grundläggande betydelse för Sverige, som försvaret, det demokratiska statsskicket, rättsväsendet och samhällsviktig verksamhet som är av betydelse ur ett nationellt perspektiv.[299]

Säkerhetsskydd
Säkerhetsskydd handlar om att skydda den information och de verksamheter som är av betydelse för Sveriges säkerhet mot spionerі, sabotage, terroristbrott och vissa andra hot. Det handlar även om att skydda verksamhet som omfattas av ett för Sverige förpliktigande internationellt åtagande om säkerhetsskydd. Utöver att skydda verksamhet och säkerhetsskyddsklassificerade uppgifter handlar säkerhetsskydd även om att skydda anläggningar, objekt, system, egendom och andra tillgångar som kan vara skyddsvärden av betydelse för Sveriges säkerhet. Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen, eller som skulle ha omfattats av den lagen om den varit tillämplig i den aktuella verksamheten.[300]

Säkerhetsskyddsåtgärder
Arbetet med säkerhetsskydd börjar med en säkerhetsskyddsanalys. I den utreder verksamheten vad som ska skyddas, mot vad och vilka åtgärder som behöver göras. Säkerhetsskyddsåtgärder kan delas in i tre huvudområden: personalsäkerhet, fysisk säkerhet och informationssäkerhet.[301]

Säkerhetsåtgärder
För att skydda information krävs säkerhetsåtgärder, det vill säga åtgärder för att möta en organisations risker. Säkerhetsåtgärder för informationssäkerhet omfattar åtgärder inom det organisatoriska, personrelaterade, tekniska och fysiska säkerhetsområdet. Åtgärderna kan verka förebyggande, upptäckande eller korrigerande. Inom det *organisatoriska området* återfinns exempelvis policyer och riktlinjer, interna rutiner och instruktioner, roll- och ansvarsfördelning, ledningens ansvar samt hantering av informationssäkerhetsincidenter. *Personrelaterade åtgärder* inbegriper bland annat bakgrundskontroll samt medvetenhet och utbildning inom

299 Säkerhetspolisen, ”Om säkerhetsskydd”, hämtad 2023-11-12.
300 Säkerhetspolisen, mejl med synpunkter på rapportutkast från Riksrevisionen, 2023-10-26.
301 Säkerhetspolisen, ”Säkerhetsskyddsåtgärder”, hämtad 2023-11-12.

informationssäkerhet. *Tekniska säkerhetsåtgärder* avser bland annat åtkomsträttigheter, säkerhetskopiering av information, inloggning, brandväggar, kryptering och antivirusskydd. Med *fysiska säkerhetsåtgärder* avses exempelvis fysiskt skalskydd och tillträde, arbete i säkrade utrymmen och placering och skydd av utrustning.[302]

Tillgänglighet
Innebär i informationssäkerhetssammanhang att en informationstillgång är åtkomlig och användbar inom förväntad tid och omfattning.

[302] Svenska institutet för standarder, Svensk standard SS-ISO/IEC 27002:2022, *Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder (ISO/IEC 27002:2022, IDT)*, utgåva 3.

Referenslista

Litteratur

Ander, T., *Informationssäkerhetskultur. Hur du bygger en säkrare organisation i en digital tidsålder*, Pug förlag, 2022.

Esaiasson, P., Gilljam, M., Oskarsson, H. och Wängnerud, L, *Metodpraktikan*, 3 uppl., Norstedts Juridik, 2010.

Hallberg, J. m.fl. (red), *Informationssäkerhet och organisationskultur*, Studentlitteratur, 2017.

Norén, K. och Wallin, M., *Akademisk chef – hur fungerar det?*, 2 uppl., Studentlitteratur, 2022.

Artiklar

Eliasson, P-O., ”Ökade hot mot lärosätena: ’Behov att växla upp säkerheten’”, *Universitetsläraren*, 2021-10-06, https://universitetslararen.se/2021/06/10/okade-hot-mot-larosatena-behov-att-vaxla-upp-sakerheten/#:~:text=S%C3%A4po%20varnade%20nyligen%20f%C3%B6r%20ett,att%20m%C3%B6ta%20de%20nya%20hoten, hämtad 2022-05-23.

Hellerstedt, L., ”Spioneriet mot svenska lärosäten fortsätter öka”, 2023-03-09, *Universitetsläraren”*, https://universitetslararen.se/2023/03/09/spioneriet-mot-svenska-larosaten-fortsatter-oka/, hämtad 2023-10-11.

Mannberg-Zackari, C., ”Fler citeringar med återbruk av data”, *Curie*, 2012-08-20, https://www.tidningencurie.se/nyheter/fler-citeringar-med-aterbruk-av-data, hämtad 2023-11-14.

Nilsson, J., ”Kinas hemliga avtal med studenter i Sverige – kräver lojalitet med regimen”, *Dagens Nyheter*, 2023-01-12.

Olsson, J., ”Cyberattacker mot universitet ökar”, Lunds universitet, 2021-10-07, https://www.lu.se/artikel/cyberattacker-mot-universitet-okar, hämtad 2022-05-23.

Skarsgård, K., ”Nätverk ska förebygga spionage mot lärosäten”, *Universitetsläraren*, 2020-02-06, https://universitetslararen.se/2020/02/06/natverk-ska-forebygga-spionage-mot-larosaten/, hämtad 2022-05-23.

Sveriges television, ”Attacker mot svenska universitets hemsidor”, *Sveriges television*, https://www.svt.se/nyheter/inrikes/storningar-pa-svenska-universitets-hemsidor, 2023-02-11, hämtad 2023-10-11.

TT, ”Säpo: Underrättelsehoten mot lärosäten ökar”, *Dagens Nyheter*, 2021-05-21.

Utredningar och rapporter m.m.

Blekinge tekniska högskola, *Riskhantering vid BTH, verksamhetsanalys och riskkostnadsberäkning avseende 2021/2022*, BTH-1.2.4-140-2022.

Blekinge tekniska högskola, *Årsredovisning 2022*, 2023.

Ernst & Young, *Granskning av informationssäkerhet på KTH*, juni 2004.

Inspektionen för strategiska produkter, *Projektrapport – universitetsprojektet*, dnr 2022-6.1-0001, 2022-12-29.

Kungl. Tekniska högskolan, Internrevisionen, *Arbetet med informationssäkerhet vid KTH*, Internrevisionsrapport 1/2014, 2014-10-17.

Kungl. Tekniska högskolan, Internrevisionen, *Granskning av KTH:s ledningssystem för informationssäkerhet*, Revisionsrapport 1/2020, 2020-10-01.

Kungl. Tekniska högskolan, *KTH:s risker 2022, riskanalys 2021*, dnr. V-2021-088, 2022-01-17.

Kungl. Tekniska högskolan, *KTH:s riskanalys 2022 – intern styrning och kontroll*, dnr. V-2022-0763, 2023-01-18.

Kungl. Tekniska högskolan, *Årsredovisning 2022*, 2023.

Lunds universitet, *Riskarbetet 2022*, dnr STYR 2022/1659.

Lunds universitet, Internrevisionen, *Årsrapport från internrevisionen år 2003*, dnr. I 6 690/2004, 2004-02-06.

Lunds universitet, Förvaltningschefen, *Kommentar till årsrapport från internrevisionen 2003*, dnr. I 6 690/2004, 2004-02-11.

Lunds universitet, *Svar på revisionsrapport 2010-01-22 granskning av intern styrning och kontroll av informationssäkerheten vid Lunds universitet*, 2010-04-21.

Lunds universitet, Internrevisionen, *Styrning av informationssäkerhet*, dnr STYR 2014/574, 2014-06-19.

Lunds universitet, Internrevisionen, *Granskning av cyber- och informationssäkerhet*, dnr STYR 2019/2167, 2019-12-13.

Lunds universitet, Internrevisionen, *Granskning av fysisk säkerhet i IT-utrymmen*, dnr STYR 2022/2678, 2022-12-20.

Lunds universitet, *Årsredovisning 2022*, 2023.

Malmö universitet, Internrevisionen, *Granskning av IT-säkerhetskultur vid Malmö universitet*, dnr LED 2022/1178, 2022-12-01.

Myndigheten för samhällsskydd och beredskap, *Konsekvensutredning för föreskrift om krav på informationssäkerhet*, 2009-11-24.

Myndigheten för samhällsskydd och beredskap, *Ledningens roll inom informationssäkerhet. Stöd för dig med en ledande funktion. Ledningens genomgång*, 2021.

Myndigheten för samhällsskydd och beredskap, *När kriget kom nära. Årsrapport it-incidentrapportering 2022*, 2022a.

Myndigheten för samhällsskydd och beredskap, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen, Resultatredovisning Infosäkkollen 2021*, 2022b.

Myndigheten för samhällsskydd och beredskap och Riksarkivet, *Vägledning för processorienterad informationskartläggning*, 2012.

PwC, Luleå tekniska universitet, *Internrevision 2021, Informationssäkerhet*, 2021-04-21.

PwC, Stockholms universitet, *Granskning av informationssäkerhet*, november 2020.

Riksrevisionen, *Granskning av intern styrning och kontroll av informationssäkerheten vid Blekinge tekniska högskola 2009*, 2010-01-26.

Riksrevisionen, *Granskning av intern styrning och kontroll av informationssäkerheten vid Lunds universitet 2009*, 2010-01-22.

Riksrevisionen, *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig*, (RiR 2023:8), 2023.

SOU 2015:92, *Utvecklad ledning av universitet och högskolor, Betänkande av Ledningsutredningen*.

SOU 2018:3, *En strategisk agenda för internationalisering. Delbetänkande av Utredningen om ökad internationalisering av universitet och högskolor*.

SOU 2021:65, *Stärkt fokus på framtidens forskningsinfrastruktur. Slutbetänkande av utredningen om organisation, styrning och finansiering av forskningsinfrastruktur*.

SOU 2021:97, *Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift. Slutbetänkande av It-driftsutredningen*.
SE/RA/326692/volym 1–9. Enkätsvar från 12 lärosäten.

Stiftelsen för internationalisering av högre utbildning och forskning, *Responsible internationalisation: Guidelines for reflection on international academic collaboration*, R20:01.

Sveriges universitets- och högskoleförbund, *Reviderad rekommendation för datahanteringsplan*, REK 2018:1 REV, dnr. 0005-17, 2019-06-26.

Sveriges universitets- och högskoleförbund, *Rekommendation om tillämpning av regelverk angående gallring och bevarande av forskningsinformation*. Antagen av SUHF:s styrelse den 2022-04-26.

Sveriges universitets- och högskoleförbund, *Vägledning med åtgärdsförslag för implementering av färdplan för öppen vetenskap. Sammanställning enkät 2023*, SUHF, Forskningsdatagruppen, 2023.

Sveriges universitets- och högskoleförbund, *Vägledning för implementering av färdplan för öppen vetenskap*, dnr SU-850-0005-17, 2022-06-30.

Säkerhetspolisen, *Säkerhetspolisen 2020*, 2021.

Universitetskanslersämbetet, *Universitet och högskolor. Årsrapport 2023*, 2023.

Uppsala universitet, Internrevisionsrapport, *Informationssäkerhetsarbete*, UFV 2021/1794, 2021-12-14.

Vetenskapsrådet, *Vägledning för implementering av kriterier för FAIR forskningsdata*, 2021.

Vetenskapsrådet, *Vägledning till mallen för datahanteringsplaner*, 2022.

Vetenskapsrådet, *Indikatorer för öppen tillgång till forskningsdata*, 1 mars 2023.

Vetenskapsrådet, *Öppen tillgång till forskningsdata 2023. En kartläggning, analys och bedömning*, 2023.

Riksdagstryck

Prop. 2001/02:158, *Samhällets säkerhet och beredskap*, bet. 2001/02:FÖU10, rskr. 2001/02:261.

Prop. 2009/10:149, *En akademi i tiden – ökad frihet för universitet och högskolor*.

Prop. 2011/12:1, *Budgetpropositionen för 2012,* utg.omr. 16, bet. 2011/12:UbU1, rskr. 2011/12:98.

Prop. 2012/12:30, *Forskning och innovation,* bet. 2012/13:UbU3, rskr. 2012/13:51.

Prop. 2016/17:50, *Kunskap i samverkan – för samhällets utmaningar och stärkt konkurrenskraft,* bet. 2016/17:UbU12, rskr. 2016/17:208.

Prop. 2020/21:1, *Budgetpropositionen för 2021*, utg.omr. 2, bet. 2020/21:FiU2, rskr. 2020/21:150

Prop. 2020/21:60, *Forskning, frihet, framtid - kunskap och innovation för Sverige,* bet. 2020/21:UbU16, rskr. 2020/21:254.

Prop. 2022/23:1, *Budgetpropositionen för 2023,* utg.omr. 16

Prop. 2023/24:1, *Budgetpropositionen för 2024,* utg.omr. 16.

Regeringsbeslut m.m.

Dir. 2019:50, Justitiedepartementet, *Ett system för granskningar av direktinvesteringar inom skyddsvärda områden*.

Dir. 2020:52, Utbildningsdepartementet, *Organisation, styrning och finansiering av forskningsinfrastruktur*.

Dir. 2023:91, Justitiedepartementet, *En förbättrad process för säkerhetsprövningar*.

Regeringsbeslut U2018/04692, U2019/02262 (delvis), U2019/03982 (delvis) m.fl., *Regleringsbrev för budgetåret 2022 avseende Kungl. Tekniska högskolan*

Regeringsbeslut U2019/02262 (delvis), U2020/03817 (delvis), U2021/04172 m.fl., *Regleringsbrev för budgetåret 2022 avseende Lunds universitet*

Regeringsbeslut Ju2019/03057/SSK, *Uppdrag till Myndigheten för samhällsskydd och beredskap att genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor*.

Regeringsbeslut Ju2019/03058/SSK, Ju2019/02421/SSK, *Uppdrag till Myndigheten för samhällsskydd och beredskap att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen*.

Regeringsbeslut U2021/04264, U2021/04851 (delvis), U2021/04907, *Regleringsbrev för budgetåret 2022 avseende Blekinge tekniska högskola*

Regeringsbeslut U2021/04851 (delvis), U2021/04891, *Regleringsbrev för budgetåret 2022 avseende universitet och högskolor*.

Regeringsbeslut U2022/02763, U2022/02805, U2022/02810 m.fl., *Regleringsbrev för budgetåret 2023 avseende universitet och högskolor*.

Regeringsbeslut U2023/02127, *Uppdrag att främja ansvarsfull internationalisering vid utbildnings-, forsknings- och innovationssamarbeten*.

Regeringskansliet, Näringsdepartementet, *Nationell inriktning för artificiell intelligens,* N2018.14.

Regeringskansliet, Utbildningsdepartementet, Ministern för högre utbildning och forskning, *Vikten av ett systematiskt säkerhetsarbete,* U2020/03059/UH, 2020-05-06.

Regeringskansliet, Utbildningsdepartementet, *Uppdrag att ta fram förslag om hur universitets och högskolors kompetens i säkerhetsfrågor kan öka*, U2023/02485, 2023-08-31.

Regeringskansliet, Utbildningsdepartementet, *Inbjudan till myndighetsdialog med Utbildningsdepartementet*, U2020/03392/UH, 2020-05-19.

Regeringskansliet, Utbildningsdepartementet, *Dagordning för myndighetsdialog med Blekinge tekniska högskola onsdagen den 21 april kl. 10.30-12.00*, U2021/00877, 2021-04-20.

Regeringskansliet, Utbildningsdepartementet, *Dagordning för myndighetsdialog med Blekinge tekniska högskola onsdagen den 18 maj kl.10.00-11.30,* U2022/, 2022-05-18.

Regeringskansliet, Utbildningsdepartementet, *Dagordning för myndighetsdialog med Kungl. Tekniska högskolan tisdagen den 27 april kl.15.30-17.00,* U2021/00877, 2021-02-22.

Regeringskansliet, Utbildningsdepartementet, *Dagordning för myndighetsdialog med Kungl. Tekniska högskolan måndagen den 30 maj kl. 13.15–14.45*, 2022-05-23.

Regeringskansliet, Utbildningsdepartementet, *Dagordning för myndighetsdialog med Lunds universitet måndagen den 29 april kl 15.00-16.30*, U2019/00361/UH, 2019-04-29.

Regeringskansliet, Utbildningsdepartementet, *Dagordning för myndighetsdialog med Lunds universitet onsdagen den 2 juni kl. 09.00-10.30,* U2021/00877, 2021-04-13.

Regeringskansliet, Utbildningsdepartementet, *Dagordning för myndighetsdialog med Lunds universitet måndagen den 11 april kl.14.00-15.30*, 2022-04-11.

Skr. 2017/18:259, Utbildningsdepartementet, *En strategi för svensk rymdverksamhet*.

Skr. 2019/20:18, Utrikesdepartementet, *Arbete i frågor som rör Kina*.

Författningar m.m.

Arkivförordning (1991:446).

Arkivlag (1990:782).

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning.

Europaparlamentets och rådets förordning (EU) 2021/821 av den 20 maj 2021 om upprättande av en unionsordning för kontroll av export, förmedling, transitering och överföring av samt tekniskt bistånd för produkter med dubbla användningsområden (omarbetning) (OJ L 206 11.06.2021).

Förordning (1993:221) för Sveriges lantbruksuniversitet.

Förordning (2000:1217) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd.

Förordning (2007:1164) för Försvarshögskolan.

Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

Förordning (2009:975) med instruktion för Vetenskapsrådet.

Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Förordning (2022:524) om statliga myndigheters beredskap.

Högskoleförordning (1993:100).

Högskolelag (1992:1434).

Internrevisionsförordning (2006:1228).

Kommissionens rekommendation (EU) 2021/1700 av den 15 september 2021 om interna efterlevnadsprogram för kontroll av forskning om produkter med dubbla användningsområden enligt Europaparlamentets och rådets förordning (EU) 2021/821 om upprättande av en unionsordning för kontroll av export, förmedling, transitering och överföring av samt tekniskt bistånd för produkter med dubbla användningsområden.

Lag (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd.

Lag (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen.

Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Lag (2022:818) om den offentliga sektorns tillgängliggörande av data.

Myndighetsförordning (2007:515).

Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10).

Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1).

Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).

Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av it-incidenter för statliga myndigheter (MSBFS 2020:8).

Offentlighets- och sekretesslag (2009:400).

Riksarkivets föreskrifter och allmänna råd om gallring av handlingar i statliga myndigheters forskningsverksamhet (RA-FS 1999:1).

Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1).

Säkerhetsskyddsförordning (2021:955).

Säkerhetsskyddslag (2018:585).

Tryckfrihetsförordning (1949:105).

Verket för förvaltningsutvecklings föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte (VERVAFS 2007:2).

Webbsidor

Inspektionen för strategiska produkter, *Introduktion till produkter med dubbla användningsområden*, https://isp.se/pda/introduktion-till-pda/, hämtad 2023-08-16.

IT-chefsforum, ”ITCF i korthet”, http://itcf.se/, hämtad 2023-10-04.

Karolinska institutet, ”Datahanteringsplaner”, https://medarbetare.ki.se/datahanteringsplaner, hämtad 2023-09-17.

KTH, ”Avtalshantering”, https://intra.kth.se/forskning/overgripande-stod/avtalshantering-1.617388, hämtad 2023-09-05.

KTH, ”Forskningsstöd vid KTH”, https://intra.kth.se/styrning/kths-organisation/vs/rso/forskningsstod-1.876021#:~:text=Forskningsst%C3%B6d%20%28RSO%29%20erbjuder%20st%C3%B6d%20till%20KTH%3As%20forskare%2C%20ledning,p%C3%A5%20KTH%20och%20i%20samverkan%20med%20externa%20partner, hämtad 2023-10-06.

KTH, ”KTH:s organisation”, https://www.kth.se/om/organisation, hämtad 2023-10-02.

KTH, ”Lediga jobb, CISO – informationssäkerhetsspecialist till KTH”, https://www.kth.se/om/work-at-kth/lediga-jobb/what:job/jobID:654035/type:job/where:4/apply:1, hämtad 2023-09-10.

KTH, ”Så bygger hon KTH:s nya säkerhetsavdelning”, https://intra.kth.se/aktuellt/nyheter/sa-bygger-hon-kth-s-nya-sakerhetsavdelning-1.1258475, hämtad 2023-08-27.

KTH, ”KTH:s verksamhetsstöd (VS)”, https://www.kth.se/om/organisation/vs-1.887371, hämtad 2023-10-02.

Lunds universitet, ”Informationssäkerhetsbloggen, Ledningssystem för informationssäkerhet har beslutats av rektor”, https://infosak.blogg.lu.se/ledningssystem-for-informationssakerhet-har-beslutats-av-rektor/, hämtad 2023-09-06.

Lunds universitet, ”Ledning och organisation”, https://www.lu.se/sites/www.lu.se/files/2021-07/organisationsschema-lunds-universitet-juli-2021.jpg, hämtad 2023-10-02.

Lunds universitet, ”Stöd till forskning vid LU” https://www.medarbetarwebben.lu.se/forska-och-utbilda/stod-till-forskning#:~:text=Hos%20Forskningsservice%20kan%20forskare%20och%20forskargrupper%20f%C3%A5%20st%C3%B6d,universitet%20kan%20ans%C3%B6ka%20om%20fakulteternas%20rese-%20och%20forskningsbidrag, hämtad 2023-09-10.

Lunds universitet, ”Universitetets förvaltning”, https://www.lu.se/om-universitetet/ledning-och-organisation/universitetets-forvaltning, hämtad 2023-10-02.

Malmö universitet, ”Forskarstöd vid Malmö universitet”, https://medarbetare.mau.se/for-ditt-arbete/forskarstod/, hämtad 2023-10-06.

Myndigheten för digital förvaltning, ”Vägledning för att tillgängliggöra information”, https://www.digg.se/kunskap-och-stod/oppna-och-delade-data/offentliga-aktorer/vagledning-for-att-tillgangliggora-information, hämtad 2023-09-15.

Myndigheten för samhällsskydd och beredskap, ”Infosäkkollen”, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/infosakkollen/, hämtad 2023-10-09.

Myndigheten för samhällsskydd och beredskaps metodstöd för systematiskt informationssäkerhetsarbete, informationssäkerhet.se, ”Klassningsmodell”, https://www.informationssakerhet.se/siteassets/metodstod-for-lis/1.-om-metodstodet/vagledning-utforma-klassningsmodell_kommentarsperiod.pdf, hämtad 2023-05-05.

Myndigheten för samhällsskydd och beredskaps metodstöd för systematiskt informationssäkerhetsarbete, informationssäkerhet.se, ”Metodstöd”, https://www.informationssakerhet.se/metodstodet/metodstodet/#:~:text=A%3A%20Metodst%C3%B6det%20f%C3%B6r%20systematiskt%20informationss%C3%A4kerhetsarbete%20%C3%A4r%20en%20samling,f%C3%B6rutom%20v%C3%A4gledningar%20och%20verktyg%2C%20r%C3%A5d%2C%20tips%20och%20mallar, hämtad 2023-03-21.

Myndigheten för samhällsskydd och beredskaps metodstöd för systematiskt informationssäkerhetsarbete, informationssäkerhet.se, ”Nätverk för offentliganställda”, https://www.informationssakerhet.se/kompetensutveckling/natverk-for-offentliganstallda/#:~:text=F%C3%B6r%20myndigheter-%20Snits.%20Snits%20%C3%A4r%20det%20statliga%20n%C3%A4tverket,erfarenhetsutbyte%2C%20kompetensutveckling%2C%20informationsspridning%20och%20diskussioner%20om%20systematiskt%20, hämtad 2023-10-03.

Myndigheten för samhällsskydd och beredskap, ”Rådgivningstjänst för systematiskt informationssäkerhetsarbete”, https://www.msb.se/sv/verktyg--tjanster/radgivningstjanst-for-systematiskt-informationssakerhetsarbete/, hämtad 2023-09-18.

Myndigheten för samhällsskydd och beredskap, “Termbanken för informationssäkerhet”, https://termbanken.informationssakerhet.se/, hämtad 2022-11-09, 2023-02-10, 2023-09-14, 2023-09-19.

Myndigheten för samhällsskydd och beredskaps metodstöd för systematiskt informationssäkerhetsarbete, informationssäkerhet.se, ”Utforma, CISO-rollen, Mandat som CISO”, https://www.informationssakerhet.se/metodstodet/utforma/#mandat-som-ciso, hämtad 2023-10-30.

MSB:s metodstöd för systematiskt informationssäkerhetsarbete, informationssäkerhet.se, ”Utforma, CISO-rollens organisatoriska placering”, https://www.informationssakerhet.se/metodstodet/utforma/#mandat-som-ciso, hämtad 2023-09-19.

Myndigheten för samhällsskydd och beredskaps metodstöd för systematiskt informationssäkerhetsarbete, informationssäkerhet.se, ”Vägledning, Klassning av information”, https://www.informationssakerhet.se/metodstodet/anvanda/#klassning-av-information, hämtad 2023-10-30.

Statistiska centralbyrån, ”Standard för svensk indelning av forskningsämnen”, https://www.scb.se/dokumentation/klassifikationer-och-standarder/standard-for-svensk-indelning-av-forskningsamnen/#:~:text=Forsknings%C3%A4mnena%20i%20OECD%3As%20klassifikation,samh%C3%A4llsvetenskap%20samt%20humaniora%20och%20kons, hämtad 2022-11-09.

Statistiska centralbyrån, ”Totala utgifter för egen FoU-verksamhet efter sektor, typ av utgift och år, 2022”, https://www.statistikdatabasen.scb.se/pxweb/sv/ssd/START__UF__UF0301__UF0301A/FoUuSvutg/table/tableViewLayout1/, hämtad 2023-11-14.

Statistiska centralbyrån, ”Universitets- och högskolesektorns utgifter för egen FoU efter lärosäte, typ av utgift och forskningsämnesområde. Mnkr, vartannat år 1993–2021, https://www.statistikdatabasen.scb.se/pxweb/sv/ssd/START__UF__UF0301__UF0301U/UoHUtgLaroAmne/, hämtad 2022-11-01 och 2023- 05-25.

Statistiska centralbyrån, Statistiknyhet från SCB 2023-07-13, ”Ökad FoU-verksamhet i Sverige under 2022”, https://www.scb.se/hitta-statistik/statistik-efter-amne/utbildning-och-forskning/forskning/forskning-och-utveckling-i-sverige/pong/statistiknyhet/forskning-och-utveckling-i-sverige-2022---preliminar-statistik/, hämtad 2023-11-13.

Stiftelsen för internationalisering av högre utbildning och forskning “STINT-internationaliseringsindex”, https://www.stint.se/stint-internationaliseringsindex/#:~:text=STINT%20internationaliseringsindex%20visar%20hur%20internationella%20svenska%20l%C3%A4ros%C3%A4ten%20%C3%A4r,som%20har%20substantiell%20forskningsvolym%20och%20det%20uppdateras%20%C3%A5rligen, hämtad 2023-09-18.

Sveriges universitetsdatanätverk, ”Anslutna organisationer”, https://www.sunet.se/om-sunet/anslutna-organisationer, hämtad 2023-11-12.

Sveriges universitetsdatanätverk, ”Datahanteringsplan”, https://www.sunet.se/services/molnbaserade-tjanster/sunet-datahanteringsplan, hämtad 2023-11-15.

Sveriges universitetsdatanätverk, ”Tjänster”, https://www.sunet.se/services, hämtad 2023-09-29.

Sveriges universitets- och högskoleförbund, ”Arbetsgruppen för informationssäkerhet och IT-/cybersäkerhet”, https://suhf.se/arbetsgrupper/arbetsgrupp-informationssakerhet-it-cybersakerhet/, hämtad 2023-10-04.

Säkerhetspolisen, ”Om säkerhetsskydd”, https://sakerhetspolisen.se/verksamheten/sakerhetsskydd/om-sakerhetsskydd.html#:~:text=S%C3%A4kerhetsk%C3%A4nslig%20verksamhet%20%C3%A4r%20s%C3%A5dan%20verksamhet,f%C3%B6rpliktande%20internationellt%20%C3%A5tagande%20om%20s%C3%A4kerhetsskydd, hämtad 2023-11-12.

Säkerhetspolisen, ”Säkerhetsskyddsåtgärder”, https://sakerhetspolisen.se/verksamheten/sakerhetsskydd/sakerhetsskyddsatgarder.html, hämtad 2023-11-12.

Säkerhetspolisen, ”Vägledningar säkerhetsskydd”, https://sakerhetspolisen.se/verksamheten/sakerhetsskydd/vagledningar-sakerhetsskydd.html, hämtad 2023-10-30.

Umeå universitet, ”Informationssäkerhet”, https://www.aurora.umu.se/stod-och-service/rad-och-riktlinjer/sakerhet/informationssakerhet/, hämtad 2023-09-08.

Universitetskanslersämbetet, ”Så styrs högskolesektorn”, https://www.uka.se/sa-fungerar-hogskolan/sa-styrs-hogskolesektorn, hämtad 2023-09-05.

Uppsala universitet, ”Datahanteringsplan (DHP)”, https://mp.uu.se/sv/web/info/forska/forskningsdata/planera/datahanteringsplan, hämtad 2023-09-05.

Utbildningsdepartementet, ”Pressmeddelande Nya styrelser för 30 universitet och högskolor”, 2023-04-27, https://www.regeringen.se/pressmeddelanden/2023/04/nya-styrelser-for-30-universitet-och-hogskolor/, hämtad 2023-09-17.

Vetenskapsrådet, ”Tillgängliggörande av forskningsdata och FAIR-kriterier”, https://www.vr.se/uppdrag/oppen-vetenskap/oppen-tillgang-till-forskningsdata/praktiskt-stod/tillgangliggorande-av-forskningsdata-och-fair-kriterier.html, hämtad 2023-09-05.

Vetenskapsrådet, ”Datahanteringsplaner”, https://www.vr.se/uppdrag/oppen-vetenskap/oppen-tillgang-till-forskningsdata/datahanteringsplaner.html, hämtad 2023-05-24.

Vetenskapsrådet, ”Mall för datahanteringsplaner”, https://www.vr.se/soka-finansiering/krav-och-villkor/ta-fram-en-datahanteringsplan/mall-for-datahanteringsplaner.html, hämtad 2023-04-25.

Vetenskapsrådet, ”Ta fram en datahanteringsplan”, https://www.vr.se/soka-finansiering/krav-och-villkor/ta-fram-en-datahanteringsplan.html, hämtad 2023-04-25.

Övrigt

Blekinge tekniska högskola, *Arbetsordning för Blekinge tekniska högskola*, dnr. BTH-1.1.3-0234-2022, 2022-10-01.

Blekinge tekniska högskola, *Information med anledning av Riksrevisionens rapport ”Granskning av intern styrning och kontroll av informationssäkerheten vid Blekinge tekniska högskola 2009”*, 2010-03-01.

Blekinge tekniska högskola, *Rektors delegationsordning, Blekinge tekniska högskola*, dnr BTH-1.1.2-0039-2021, 2021-02-10.

Blekinge tekniska högskola, *Riktlinjer för informationssäkerhet vid Blekinge Tekniska Högskola*, version 1.0, dnr 130-0951-2012, 2012-06-19.

European Commission, Horizon Europe (HORIZON) Programme Guide, Version 3.0, 1 April 2023.

Högskolan i Borås, *Ansvar och roller i ledningssystem för Informationssäkerhet (LIS) vid Högskolan i Borås*, dnr 151-22, 2022-05-04.

It-säkerhetsnätverket, *Sektorsgemensam återkoppling Vägledning säkerhetsåtgärder i informationssystem v. 0.2*, 2022-04-13.

KTH, *Arbetsordning vid KTH*, Förskrift beslutad av universitetsstyrelsen, dnr V-2019-0561, senast ändrad genom V-2022-0691, gäller från och med 2019-07-01, senast ändrad från och med 2023-01-01.

KTH, *Arbets- och delegationsordning för verksamhetsstödet vid KTH*, beslutsfattare universitetsdirektören, dnr V-2021-0484, ändrad genom V-2022-0780, gäller från och med 2021-06-21, ändrad från och med 2023-01-01.

KTH, *Anvisning för informations- och IT-säkerhet*, 2014-02-01.

KTH, *Anvisning Informationsklassificering för KTH*, Riktlinje gäller från och med 2015-01-01

KTH, *Delegationsordning för KTH*, gäller från och med 2023-01-01.

KTH, KTH:s remissvar *Förslag till Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet och föreskrifter om it-säkerhet för statliga myndigheter, 2019-14545/2019-14546*, V-2019-1176, 2020-02-11.

Lunds universitet, *Arbetsordning för Lunds universitet*, fastställd av universitetsstyrelsen 2018-12-14, § 12, reviderad av universitetsstyrelsen 2022-10-28 § 11, dnr. STYR 2018/1859, STYR 2019/907, STYR 2019/1903, STYR 2020/2283, STYR 2021/2702, STYR 2022/1481, 2022-10-28.

Lunds universitet, *Föreskrifter om fördelning av beslutsbefogenheter inom universitetsförvaltningen vid Lunds universitet*, dnr STYR 2021/726, 2021-05-11.

Lunds universitet, *Ledningssystem för informationssäkerhet vid Lunds universitet*, dnr STYR 2022/587, fastställd av rektor 2022-03-24.

Lunds universitet, *Lunds universitets föreskrifter om fördelning av beslutsbefogenheter och rätt att teckna avtal vid Lunds universitet,* dnr STYR 2022/1382, 2022-06-09.

Lunds universitet, *Riktlinjer för informationssäkerhet vid Lunds universitet,* dnr STYR 2017/947, rektors beslut, 2017-06-22.

Lunds universitet, Sektionen Externa relationer, *Checklista för Globalt ansvarsfullt engagemang*, mars 2023.

Lunds universitet, *Uppföljning av Yttrande över Internrevisionens rapport "Styrning av informationssäkerhet"*, 2019-10-11.

Svensk nationell datatjänst, *Checklista för datahanteringsplan*, Version 12, 2021-01-26.

Svenska institutet för standarder, *Svensk standard SS-EN ISO/IEC 27000:2020 Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Översikt och terminologi (ISO/IEC 27000:2018)*, utgåva 2.

Svenska institutet för standarder, *Svensk standard SS-ISO/IEC 27002:2022, Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder (ISO/IEC 27002:2022, IDT)*, utgåva 3.

Sveriges universitetsdatanätverk, *Protokoll fört vid kommittésammanträdet 2023-06-01.*

Sveriges universitets- och högskoleförbund, "Information från SUHF angående säkerhetsutbildning i sektorn", mejl till universitet och högskolor, 2020-05-07.

Bilaga 1. Granskningsdesign och metod

För att svara på den övergripande revisionsfrågan med underliggande delfrågor har vi använt en kombination av intervjuer, dokumentstudier och en enkätundersökning. Vi har även gått igenom relevant rättspraxis och diverse rapporter inom ämnet. Nedan redogör vi för de metoder för datainsamling och analys som vi använt och de urval vi gjort i granskningen.

Urval

24 lärosäten med naturvetenskaplig och teknisk forskning

Granskningen är avgränsad till de 24 statliga lärosäten som år 2021 bedrev forskning inom forskningsämnesområdena naturvetenskap och/eller teknik. Urvalet baseras på Statistiska centralbyråns (SCB) statistik över *universitets- och högskolesektorns utgifter för egen FoU efter lärosäte, typ av utgift och forskningsämnesområde*.[303] År 2021 hade 26 svenska lärosäten utgifter inom forskningsämnesområdena naturvetenskap och teknik. Två av dessa, Stiftelsen högskolan i Jönköping och Chalmers tekniska högskola Aktiebolag, är inte inkluderade i urvalet eftersom de inte är statliga lärosäten.

Tabell 1 Universitets- och högskolesektorns utgifter för egen FoU efter lärosäte och forskningsämnesområde, miljoner kronor, 2021. Sorterat efter totala utgifter för naturvetenskap och teknik (högst till lägst).

Lärosäte	Utgifter naturvetenskap	Utgifter teknik	Utgifter naturvetenskap och teknik
Kungl. Tekniska högskolan	1 012	2 331	**3 343**
Lunds universitet	1 881	926	**2 807**
Uppsala universitet	1 605	323	**1 928**
Stockholms universitet	1 920	0	**1 920**
Linköpings universitet	958	483	**1 442**
Göteborgs universitet	933	21	**953**
Luleå tekniska universitet	124	692	**816**
Umeå universitet	726	61	**787**

[303] SCB, Statistikdatabasen, ”Universitets- och högskolesektorns utgifter för egen FoU efter lärosäte, typ av utgift och forskningsämnesområde. Mnkr, vartannat år 1993–2021”, hämtad 2022-11-01.

Lärosäte	Utgifter naturvetenskap	Utgifter teknik	Utgifter naturvetenskap och teknik
Linnéuniversitetet	174	72	**246**
Mälardalens universitet	129	85	**214**
Mittuniversitetet	85	126	**212**
Örebro universitet	184	12	**196**
Karlstads universitet	126	49	**175**
Blekinge tekniska högskola	79	69	**148**
Högskolan Väst	2	137	**140**
Högskolan i Skövde	68	49	**117**
Högskolan i Gävle	17	81	**98**
Högskolan i Halmstad	45	38	**83**
Högskolan i Borås	25	53	**78**
Malmö universitet	61	10	**71**
Södertörns högskola	41	0	**41**
Högskolan Dalarna	13	23	**36**
Högskolan Kristianstad	20	4	**24**
Försvarshögskolan	0	12	**12**

Anm.: Stiftelsen högskolan i Jönköping och Chalmers tekniska högskola Aktiebolag har uteslutits från tabellen.

Vi har gjort en ämnesmässig avgränsning till forskningsämnesområdena naturvetenskap och teknik av flera anledningar. För det första är det två breda områden där flera olika skyddsvärden är aktuella. Det kan exempelvis handla om skyddsvärden relaterade till Sveriges säkerhet eller svensk innovation och konkurrenskraft. Det förekommer även skyddsvärden kopplade till samhällsviktig infrastruktur, personlig integritet och individuell säkerhet inom dessa forskningsämnesområden. Sverige är en forskningsnation i framkant i flera naturvetenskapliga och tekniska forskningsämnen och det finns ett betydande intresse för denna forskning från externa aktörer.[304]

[304] Intervju med företrädare för Säkerhetspolisen, 2022-10-20.

För det andra fick vi under granskningens förberedande fas indikationer på att informationssäkerheten generellt är mer utvecklad inom medicin och hälsovetenskap än inom naturvetenskap och teknik. En förklaring till det kan vara att det medicinska området har mer erfarenhet av att skydda känsliga personuppgifter i form av exempelvis patientdata. Av den anledningen avgränsade vi bort medicin och hälsovetenskap.

Sammantaget har vi bedömt det som mer angeläget att fokusera på informationssäkerheten inom naturvetenskap och teknik även om granskningens resultat är av relevans för samtliga forskningsämnesområden vid svenska lärosäten.

Tre exempellärosäten för intervjuer och dokumentstudier

Vi har genomfört fördjupade undersökningar av informationssäkerheten vid tre lärosäten: Blekinge tekniska högskola (BTH), Kungl. Tekniska högskolan (KTH) och Lunds universitet (LU). Inom de naturvetenskapliga och tekniska fakulteterna (eller motsvarande) på dessa tre lärosäten har vi även gjort ett urval av institutioner och forskare/forskargrupper. Djupare undersökningar på dessa tre lärosäten ger oss en bättre förståelse för hur informationssäkerhetsarbetet utformas och genomförs i praktiken på olika typer av lärosäten. Det gör det också möjligt att synliggöra de olika mekanismer som påverkar informationssäkerhetsarbetet och hanteringen av skyddsvärda forskningsdata. Syftet med urvalet är inte bara att uttala oss om de tre enskilda lärosätena vi granskar, utan att genom iakttagelser från dem kunna dra slutsatser som är relevanta för hela sektorn.

De tre lärosätena ska inte ses som ett representativt urval av de 24 lärosätena i populationen, och generaliseringar från urvalet bör därför inte göras. Vi bedömer att det finns för många okända faktorer i lärosätenas informationssäkerhetsarbete för att vi ska kunna göra tillräckligt säkra antaganden om typiska fall.[305] Lärosätena i vårt urval ska ses som exempel på hur olika typer av lärosäten kan arbeta med informationssäkerhet, och tjänar även syftet att hjälpa oss kartlägga orsaker till brister.

En avgörande princip i vårt urval av lärosäten, institutioner och forskare har således varit att fånga in så mycket variation som möjligt. Vi har därför valt tre exempellärosäten som skiljer sig åt bland annat gällande typ av lärosäte, organisationsstorlek och storlek på anslag. Vi har dessutom utgått ifrån att variationen inte bara finns mellan lärosäten utan även inom de enskilda lärosätena, givet deras decentraliserade organisation och verksamhet. Till exempel kan det även i mindre decentraliserade organisationer förekomma olikheter mellan fakulteter och

[305] Se t.ex. Esaiasson m.fl., *Metodpraktikan*, 2010, s. 165–166 om typiska fall.

institutioner i exempelvis organisation, kultur, prioriteringar och budget. Vårt urval av flera institutioner från samma lärosäte bidrar med variation bland annat gällande institutionsstorlek och ämnesområden. Därmed finns en variation även gällande olika skyddsvärden och tillämpliga lagstiftningar. På så vis får vi många och breda exempel på hur informationssäkerhetsarbete bedrivs vid lärosäten.

Från inledande intervjuer under granskningens förberedande fas fick vi indikationer även på andra faktorer som kan ha betydelse för hur informationssäkerhetsarbetet bedrivs. Det gäller till exempel kunskap bland personal, ansvarsfördelning mellan olika organisationsnivåer och funktioner, omfattning och typ av internationella samarbeten, olika finansieringsformer (till exempel grad av extern finansiering) och resurser som läggs på informationssäkerhetsarbete. Även andra faktorer kom fram, såsom varierande incitamentsstrukturer för forskare att skydda sin data, att regelverk upplevs som krångliga och inte anpassade för lärosätenas verksamhet, bristande tydlighet i styrning på olika nivåer och målkonflikter mellan öppen vetenskap och skydd av forskningsdata. Vårt urval av tre lärosäten har tillåtit oss att undersöka många av dessa faktorer och kontexter, likväl som andra inledningsvis okända faktorer.

Givet variationen i vårt urval finns det god anledning att anta att våra slutsatser är generellt relevanta och intressanta även för andra lärosäten, även om iakttagelserna från våra tre exempellärosäten alltså inte är direkt generaliserbara.

Totalt ingick 3 lärosäten, 9 fakulteter och 21 institutioner i vårt urval i den fördjupade undersökningen. Institutionerna täcker in områden som exempelvis biologi, bioteknologi, datavetenskap, energiteknik, energivetenskap, fysik, hållbar utveckling, kemiteknik, maskinteknik, materialvetenskap och teknisk mekanik.

Tabell 2 Lärosäten och fakulteter som ingår i Riksrevisionens fördjupade undersökning

Blekinge tekniska högskola	Fakulteten för datavetenskaper Fakulteten för teknikvetenskaper
Kungl. Tekniska högskolan	Skolan för arkitektur och samhällsbyggnad Skolan för elektroteknik och datavetenskap Skolan för industriell teknik och management Skolan för kemi, bioteknologi och hälsa Skolan för teknikvetenskap
Lunds universitet[306]	Lunds tekniska högskola Naturvetenskapliga fakulteten

306 Några institutioner vid Lunds universitet är organiserade under båda fakulteterna.

Metoder

Intervjuer och dokumentstudier vid tre lärosäten

Vi har genomfört sammanlagt 65 semistrukturerade intervjuer vid BTH, KTH och LU. Totalt intervjuades 119 personer i dessa intervjuer.[307] Vi intervjuade forskare, anställda inom förvaltning och verksamhetsstöd samt akademiska ledare och chefer inom förvaltningen. Se tabell 3 nedan för en sammanställning av de roller och funktioner som vi intervjuade vid de tre lärosätena.

De flesta intervjuer genomfördes med en eller två personer åt gången. Vid några intervjutillfällen deltog upp till tiotalet personer. Urvalet av intervjupersoner började med att vi genom en kartläggning identifierade nyckelpersoner i lärosätenas informationssäkerhetsarbete. Denna kartläggning kompletterades vid behov av lärosätena. De forskare vi intervjuat valdes ut dels av oss, dels på förslag av lärosätena. I urvalet av forskare strävade vi efter en spridning utifrån forskningsämne, typer av externa samarbeten och finansieringskällor samt olika skyddsvärden för de data som hanteras.

Intervjuerna genomfördes i huvudsak under första halvåret av 2023 på plats på respektive lärosäte. Ett fåtal intervjuer genomfördes digitalt via Teams eller Skiffer. Intervjuerna var semistrukturerade och vägleddes av intervjuguider som anpassades efter den anställdas roll och arbetsuppgifter. Intervjuguiderna var likadana för samma typ av roller vid de olika lärosätena. Som regel intervjuade vi inte anställda tillsammans med deras chefer, med ett fåtal undantag när det var nödvändigt för att få en förståelse för frågeställningarna. De flesta intervjuerna varade mellan 60 och 90 minuter.

De flesta intervjuer som genomfördes på plats spelade vi in med diktafon och skrev utifrån dem intervjuanteckningar. Intervjuerna kodades och analyserades sedan utifrån dels de teman vi frågade om i intervjuerna, dels andra teman som identifierades i vår analys av materialet.

[307] Denna siffra är lägre än summan av antalet personer i bilaga 2 eftersom vissa personer deltog i flera intervjuer.

Tabell 3 Intervjuade vid Blekinge tekniska högskola, Kungl. Tekniska högskolan och Lunds universitet efter roll/funktion

Roll/funktion	Blekinge tekniska högskola	Kungl. Tekniska högskolan	Lunds universitet
Förvaltningschef	1	1*	1
Dekan	2	5**	2
Prefekt	4	10	6
Forskare, inkl. doktorander	5 (1***)	4 (2***)	11 (2***)
Chief Information Security Officer	-	1	1
Informationssäkerhetssamordnare	1	-	1
Dataskyddsombud/dataskyddssamordnare	1	1	1
It-chef	1	1	1
It, övrigt (t.ex. it-säkerhetschef, it-arkitekt, it-specialist)	1	3	6
Säkerhetschef	-	-	1
Jurist	-	2	2
Bibliotek (t.ex. rådgivare/koordinator för forskningsdata)	2	2	8
Internrevision	-	3	-
Övrigt, förvaltning och verksamhetsstöd (övrig säkerhetspersonal, internationaliseringsrådgivare, rådgivare exportkontroll/PDA, exportrådgivare, forskningsrådgivare, innovationsrådgivare, administrativa chefer, utvecklingsstrateg, LUNARC[308])	5	7	5
Övrigt, akademi (vicerektor, vice skolchef, proprefekt, prorektor, vice dekan)	-	3	4

** biträdande förvaltningschef*
*** skolchef*
**** forskare som intervjuades med fokus på it-säkerhet*
Anm.: Anställda inom verksamhetsstödet som innehade flera av de specificerade rollerna har räknats en gång per roll som specificerats. Prefekter och andra akademiska ledare och chefer har inte räknats in i kategorin "forskare".

[308] Centrum för tekniska och vetenskapliga beräkningar vid Lunds universitet.

Utöver intervjuer har vi granskat olika styrdokument, interna analyser och rapporter, policyer och annan relevant dokumentation. Det gäller exempelvis delegations- och arbetsordningar, informationssäkerhetspolicyer, riskanalyser och internrevisionsrapporter. Syftet var att komplettera bilden från intervjuerna av hur informationssäkerhetsarbetet har utformats, genomförts och följts upp på lärosätena.

Enkät till 24 lärosäten

I april 2023 skickade vi ut en enkät till de 24 lärosäten som omfattas av granskningen. Enkäten bestod av två delar: en webbenkät i enkätverktyget Webropol och en kortare postenkät om säkerhetsskydd. Alla 24 lärosäten besvarade enkäten, även om vissa lärosäten lämnade några frågor obesvarade. Enkätens båda delar finns i bilaga 4.

Del 1, webbenkäten, innehöll 37 frågor om lärosätenas informationssäkerhetsarbete. Frågorna handlade om roller och styrdokument i informationssäkerhetsarbetet, inventering och klassning av information, riskbedömning och analys, informationssäkerhetsincidenter, resurser, utbildning av medarbetare samt kurser inom informationssäkerhet. Utöver det fanns det även fritextfrågor om lärosätenas prioriteringar i informationssäkerhetsarbete de senaste två åren, vad de bedömer som mest angeläget att förbättra, utmaningar samt vad de tycker fungerar bra. Del 2 av enkäten innehöll 9 frågor, med fokus på säkerhetsskydd och rutiner för skyddsvärda informationstillgångar och säkerhetskänslig verksamhet.

Innan vi skickade ut enkäten stämde vi av den vid ett möte med informationssäkerhetsstrategen och säkerhetschefen vid Sveriges lantbruksuniversitet, SLU. Syftet var att öka relevansen och försäkra oss om att frågorna var förståeliga. Inför utskick stämde vi också av enkäten med Riksrevisionens ämnessakkunniga i enkätmetodik.

Det huvudsakliga syftet med enkäten var att få en bred bild av hur lärosätena som bedriver naturvetenskaplig och teknisk forskning arbetar med informationssäkerhet. Enkätens frågeområden beslutades efter att vi vid besök och intervjuer vid BTH, KTH och LU ringat in centrala aspekter och problem i lärosätenas informationssäkerhetsarbeten. Delar av enkäten utgår även från Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

Övriga intervjuer, aktiviteter och dokumentstudier

I oktober 2022 gjorde vi ett två dagars besök vid Malmö universitet där vi intervjuade en rad funktioner. Vi besökte även RISE Research Institutes of Sweden AB i Göteborg och SLU i Uppsala i november respektive december 2022. Syftet var att öka förförståelsen för hur ett lärosäte och en forskningsorganisation arbetar med informationssäkerhet och vilka utmaningar som finns.

Vi har även tagit del av underlag från MSB:s verktyg Infosäkkollen[309] samt 2021 och 2022 års myndighetsdialoger för BTH, KTH och LU. Utöver det har vi genomfört intervjuer med företrädare för Säkerhetspolisen, MSB, Vetenskapsrådet, Länsstyrelserna Norrbotten, Skåne, Stockholm och Västra Götaland, Patent- och registreringsverket, Sveriges universitets- och högskoleförbund, Svensk nationell datatjänst, Jernkontoret och SSAB. Vi har även haft möten och intervjuer med ytterligare forskare och yrkesverksamma på lärosäten och i andra organisationer som har relevant kunskap om informationssäkerhet.

[309] Se MSB, ”Infosäkkollen”, hämtad 2023-10-09.

Bilaga 2. Intervjuer vid de tre exempellärosätena

Tabell 4 Intervjuer vid Blekinge tekniska högskola (BTH), Kungl. Tekniska högskolan (KTH) och Lunds universitet (LU), sorterade i datumordning

Referens i fotnot	Funktion/roll[310]	Datum
BTH1	It-chef, informationssäkerhetsansvarig, dataskyddsombud	2023-01-03
KTH1	Avdelningschef/bitr. universitetsdirektör, koordinator för forskningsdata, it-säkerhetschef tillika Chief Information Security Officer, systemspecialist, dataskyddsombud	2023-01-10
KTH2	Koordinator för forskningsdata och rådgivare/handläggare forskningsdata	2023-01-11
KTH3	Vicerektor internationella relationer, rådgivare forskningsetik och exportkontroll, koordinator för forskningsdata	2023-01-13
KTH4	Skolchef samt administrativ chef för Skolan för industriell teknik och management, tf skolchef samt administrativ chef för Skolan för kemi, bioteknik, hälsa, skolchef samt administrativ chef för Skolan för arkitektur och samhällsbyggnad, koordinator för forskningsdata, it-säkerhetschef tillika Chief Information Security Officer	2023-01-16
KTH5	It-chef, it-säkerhetschef tillika Chief Information Security Officer	2023-01-16
KTH6	Skolchef, vice skolchef, administrativ chef och representant från it vid Skolan för teknikvetenskap, proprefekt och prefekt, institutioner vid Skolan för teknikvetenskap, skolchef och administrativ chef för Skolan för elektroteknik och datavetenskap, koordinator för forskningsdata, it-säkerhetschef tillika Chief Information Officer	2023-01-16
KTH7	Internrevisionschef och internrevisorer	2023-01-17
KTH8	Gruppchef affärsjuridik, funktionsansvarig förvaltningsjuridik, koordinator för forskningsdata, it-säkerhetschef tillika Chief Information Officer	2023-01-17
BTH2	Högskoledirektör	2023-01-23
BTH3	Informationssäkerhetsansvarig	2023-01-23
BTH4	Forskningsrådgivare och innovationsrådgivare	2023-01-23
BTH5	Prefekter, institutioner vid fakulteten för datavetenskaper	2023-01-23
BTH6	Dekan, fakulteten för datavetenskaper och dekan, fakulteten för teknikvetenskaper	2023-01-23

[310] Avser den funktion/roll som personen hade vid intervjutillfället.

Referens i fotnot	Funktion/roll[310]	Datum
BTH7	Rådgivare forskningsdatastöd	2023-01-24
BTH8	Prefekter, institutioner vid fakulteten för teknikvetenskaper	2023-01-24
BTH9	It-arkitekt	2023-01-24
BTH10	Internationaliseringsansvarig och exportrådgivare	2023-01-24
BTH11	Forskare, institution vid fakulteten för teknikvetenskaper	2023-01-25
BTH12	Forskare, institution vid fakulteten för datavetenskaper	2023-01-25
BTH13	Forskare, institution vid fakulteten för datavetenskaper	2023-01-25
BTH14	Forskare, institution vid fakulteten för teknikvetenskaper	2023-01-25
LU1	Utvecklingsstrateg vid universitetsledningens stab för utveckling, chefsjurist, dataskyddssamordnare, utvecklingsstrateg, säkerhetschef/säkerhetshetsskyddschef, bibliotekschef för naturvetenskapliga fakulteten, säkerhetssamordnare, Chief Information Security Officer, it-direktör, avdelningschef universitetsbiblioteket, överbibliotekarie, avdelningschef på ledningsstöd	2023-02-01
BTH15	Forskare, institution vid fakulteten för datavetenskaper	2023-02-07
KTH9	Prefekter, institutioner vid Skolan för teknikvetenskap	2023-02-16
KTH10	Prefekter, institutioner vid Skolan för elektroteknik och datavetenskap	2023-02-20
KTH11	Prefekt, institution vid Skolan för kemi, bioteknologi och hälsa	2023-02-21
KTH12	Forskare, institution vid Skolan för teknikvetenskap	2023-02-22
KTH13	Prefekt, institution vid Skolan för kemi, bioteknologi och hälsa	2023-02-27
KTH14	Prefekter, institutioner vid Skolan för industriell teknik och management	2023-02-27
KTH15	Prefekt/avdelningschef och prefekt vid institutioner vid Skolan för arkitektur och samhällsbyggnad	2023-02-28
LU2	Chief Information Security Officer	2023-03-07
LU3	It-säkerhetsmedarbetare, LDC	2023-03-07
LU4	Vice rektor för forskningsinfrastruktur, digitalisering och forskarutbildning	2023-03-08
LU5	Medarbetare, universitetsbiblioteket, Open science	2023-03-08
LU6	Vice rektor för samverkan och internationella relationer	2023-03-08
LU7	Förvaltningschef	2023-03-08
LU8	Avdelningschef, universitetsbiblioteket	2023-03-08
LU9	Säkerhetschef/säkerhetsskyddschef och säkerhetssamordnare	2023-03-08

Referens i fotnot	Funktion/roll[310]	Datum
LU10	Chefsjurist och jurist, Lunds tekniska högskola och Naturvetenskapliga fakulteten	2023-03-08
LU11	Medarbetare, biblioteket Naturvetenskapliga fakulteten	2023-03-08
LU12	Medarbetare, biblioteket Lunds tekniska högskola	2023-03-08
LU13	It-medarbetare, Lunds tekniska högskola och Naturvetenskapliga fakulteten	2023-03-08
LU14	Vice dekan, Naturvetenskapliga fakulteten	2023-03-09
LU15	Prorektor, Lunds tekniska högskola	2023-03-09
LU16	Prefekter och biträdande prefekt, institutioner vid Naturvetenskapliga fakulteten	2023-03-09
LU17	Prefekter, institutioner vid Lunds tekniska högskola	2023-03-09
LU18	Forskare, institution vid Naturvetenskapliga fakulteten	2023-03-09
LU19	Forskare och doktorand, institution vid Lunds tekniska högskola	2023-03-09
LU20	Forskare, institution vid Lunds tekniska högskola	2023-03-09
LU21	Forskare, institutioner vid Lunds tekniska högskola och Naturvetenskapliga fakulteten	2023-03-09
LU22	Forskare, institutioner vid Lunds tekniska högskola och Naturvetenskapliga fakulteten	2023-03-09
LU23	Medarbetare, Centrum för tekniska och vetenskapliga beräkningar vid Lunds universitet (LUNARC)	2023-03-09
LU24	Dataskyddsamordnare, informationssäkerhetssamordnare	2023-03-09
LU25	Chief Information Security Officer och utvecklingsstrateg vid universitetsledningens stab för utveckling	2023-03-10
KTH16	Forskare, institution vid Skolan för teknikvetenskap	2023-03-16
LU26	Dekan, Naturvetenskapliga fakulteten	2023-03-21
KTH17	Forskare, institution vid Skolan för elektroteknik och datavetenskap	2023-03-22
KTH18	Forskare, institution vid Skolan för elektroteknik och datavetenskap	2023-03-22
LU27	Rektor, Lunds tekniska högskola	2023-03-27
KTH19	Forskare, institution vid Skolan för teknikvetenskap	2023-05-04
KTH20	Forskare, institution vid Skolan för elektroteknik och datavetenskap	2023-05-11
BTH16	Doktorand, institution vid fakulteten för teknikvetenskaper	2023-05-30
LU28	Forskare, centrum vid Naturvetenskapliga fakulteten	2023-06-27
LU29	Doktorand, institution vid Medicinska fakulteten	2023-08-10

Viss forskning behöver skyddas för att inte skada exempelvis individers integritet, Sveriges konkurrenskraft eller samhällets säkerhet. Antalet cyberattacker har ökat och underrättelseverksamheten mot universitet och högskolor har intensifierats under senare år. Behovet av att lärosätena bedriver ett effektivt informationssäkerhetsarbete för att skydda forskningsdata har därmed ökat.

Riksrevisionen bedömer att det fortfarande saknas väsentliga delar av ett systematiskt informationssäkerhetsarbete på lärosätena, trots att föreskriftskrav funnits sedan 2008 och bristerna varit kända sedan länge. De åtgärder som regering, lärosäten och andra berörda myndigheter hittills vidtagit har inte varit tillräckliga.

Riksrevisionen rekommenderar därför regeringen att genom olika uppdrag bistå lärosätena med mer stöd i syfte att förbättra informationssäkerhetsarbetet. Lärosätesledningarna rekommenderas att se till att alla delar i det systematiska informationssäkerhetsarbetet finns på plats.

Riksrevisionen

S:t Eriksgatan 117
Box 6181, 102 33 Stockholm
08-5171 40 00
www.riksrevisionen.se