

Informationssäkerhet vid universitet och högskolor – hanteringen av skyddsvärda forskningsdata (RiR 2023:20)

Riksrevisor: Helena Lindberg

Projektgrupp: Sara Monaco, Ludvig Stendahl och Klara Folkesson

Enhetschef: Katarina Richardson

Kort om Riksrevisionen

- En del av riksdagens kontrollmakt
- Vi bedriver oberoende revision av statliga åtaganden i syfte att:
 - Bidra till god resursanvändning och effektiv förvaltning i staten
 - Ge underlag som möjliggör för riksdagen att utkräva ansvar

Vad är effektivitetsrevision?

- Fokus på hushållning, resursutnyttjande och måluppfyllelse.
- Vi arbetar efter en fastställd process som utgår från lagstiftning och internationella standarder.
- Vi gör ungefär 30 rapporter årligen och en granskning tar cirka 1 år.
- Rapporterna överlämnas till riksdagen.
- Riksdagen överlämnar sedan rapporten till regeringen.
- Regeringen ska inom fyra månader redovisa vilka åtgärder den har vidtagit eller avser vidta med anledning av granskningen.

Motiv för granskning

- Föreskriftskrav sedan 2008 om att statliga myndigheter ska bedriva ett systematiskt informationssäkerhetsarbete.
- Cyberattacker och underrättelseverksamhet har ökat.
- Brister i lärosätenas informationssäkerhetsarbete.
- Riksdagen har uttalat att det är viktigt att Sverige har en god förmåga att skydda bland annat forskning från industrispionage.

Bedriver universitet och högskolor ett effektivt informationssäkerhetsarbete som möjliggör att skyddsvärda forskningsdata hanteras säkert och enligt gällande regelverk?

Delfrågor

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

Skyddsvärda forskningsdata

- Data som kan behöva skyddas på grund av **sekretess, dataskyddsreglering** eller **annan specialreglering**.
- Exempelvis känsliga personuppgifter, företagshemligheter eller säkerhetskänslig verksamhet.
- En övervägande del av forskningsdata kan vara öppen och tillgänglig för alla.

Avgränsningar

- De 24 lärosäten som bedriver naturvetenskaplig och teknisk forskning.
- Fokus på forskningsdata och konfidentialitet.
- Fokus på organisatorisk och administrativ säkerhet.

Hur har vi granskat?

Bedömningsgrunder

- MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6)
- MSB:s metodstöd för systematiskt informationssäkerhetsarbete
- Förordningen (2022:524) om statliga myndigheters beredskap

Hur har vi granskat? (forts.)

Metod för empiriinsamling och analys

- Intervjuer och dokumentstudier
- Tre exempellärosäten: Blekinge tekniska högskola, KTH och Lunds universitet
- Enkät till 24 lärosäten

Arbetet med att identifiera skyddsvärda forskningsdata och att analysera informationssäkerhetsrisker

- Lärosätena arbetar inte systematiskt för att inventera och klassa forskningsdata.
- Separata it-organisationer och egna it-lösningar försvårar ett sammanhållet informationssäkerhetsarbete.
- Lärosätenas riskbedömningar inkluderar sällan informationssäkerhet för forskningsdata.

Utformningen av informationssäkerhetsarbetet

- Styrningen av informationssäkerhetsarbetet har brister.
- Roll- och ansvarsfördelning är ofta otydlig.
- Medarbetarnas kompetens varierar stort.
- Stödet för säker forskningsdatahantering är inte tillräckligt ändamålsenligt.

Slutsatser

- Lärosätena arbetar inte effektivt för att identifiera skyddsvärda forskningsdata.
- Lärosätena har otillräcklig kunskap och kompetens att bedöma vad som är skyddsvärt.
- Lärosätesledningarna har inte styrt och organiserat informationssäkerhetsarbetet på ett effektivt sätt.
- Regeringens och myndigheternas åtgärder för att stärka informationssäkerhetsarbetet vid lärosätena har varit otillräckliga.

Rekommendationer till regeringen

Ge uppdrag till

- Myndigheten för samhällsskydd och beredskap att genomföra kompetenshöjande insatser till ledningarna för universitet och högskolor.
- universitet och högskolor att i samverkan inrätta en gemensam stödfunktion för informationssäkerhet.

Rekommendationer till 24 universitet och högskolor

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
- de som leder det strategiska informationssäkerhetsarbetet har mandat att ställa krav och granska informationssäkerhetsarbetet samt att de regelbundet rapporterar till lärosätesledning och styrelse.

Rekommendationer till 24 universitet och högskolor (forts.)

Se till att

- arbetssätten för informationsklassning av forskningsdata är enhetliga
- det finns kompetens att analysera informationssäkerhetsrisker kopplade till forskningsdata
- det finns ett samordnat stöd för medarbetare att hantera forskningsdata korrekt under hela livscykeln.