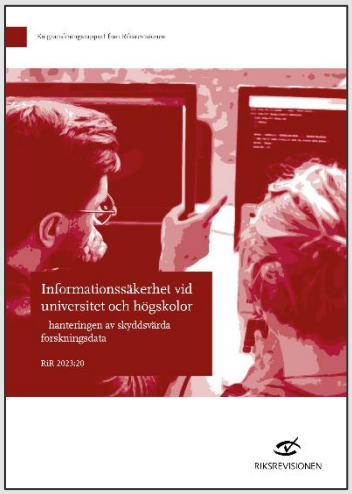
RIKSREVISIONEN

Bilaga till granskningsrapport

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

Bilaga 4
Riksrevisionens enkät om informationssäkerhet till 24 lärosäten



Informationssäkerhet vid universitet och högskolor

– hanteringen av skyddsvärda forskningsdata

Del 1

Missiv

Inom ramen för Riksrevisionens granskning ber vi er besvara en enkät om informationssäkerhetsarbetet vid lärosätet. Enkäten går ut till de 24 lärosäten som bedriver forskning inom naturvetenskap och teknik. Enkäten riktas i första hand till informationssäkerhetschef/motsvarande. Viss samordning med andra funktioner kan behövas. Frågorna avser lärosätesövergripande nivå om inte annat anges. Observera att det inte får finnas några uppgifter i svaren som omfattas av någon form av sekretess. Kontakta oss i annat fall.

Svara gärna så snart som möjligt, men allra senast den 8 maj. Vid frågor hör gärna av er till Ludvig Stendahl eller Sara Monaco.

Tack för er medverkan!

Forskningsdata avser data som samlas in eller framställs inom ramen för vetenskaplig forskningsverksamhet. Det kan t.ex. vara digitala texter, bilder, audiovisuella material, 3D-skanningar, observationsdata, resultat från experiment och andra typer av digitala objekt. Sammanfattningsvis utgörs forskningsdata av det underlag som lett fram till ett forskningsresultat.

Enkät informationssäkerhet UoH

Totala antalet respondenter: 24

Fråga 1. Vilket lärosäte företräder du?

Ange lärosäte i listan nedan.

Antal svar: 24

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

Fråga 2. Vad har du som besvarar enkäten för roll på lärosätet?

Antal svar: 24, valda alternativ: 33

	Antal	Procent
Informationssäkerhetschef/motsvarande	8	33
Annan roll, ange:	6	25
Om ni är flera som besvarar enkäten, vänligen lista alla personers tjänstebefattning:	19	79

Fråga 3. Vänligen markera samtliga av följande befattningar, roller och funktioner som finns på lärosätet.

Frågan avser roller som finns på lärosätesövergripande nivå om inte annat anges.

Antal svar: 24, valda alternativ: 292

	Antal	Procent
Informationssäkerhetschef	12	50
Informationssäkerhetsspecialist	4	17
Informationssäkerhetssamordnare/informationssäkerhetsstrateg eller motsvarande	18	75
Lokala informationssäkerhetsansvariga eller motsvarande på fakulteter eller institutioner (lokal kontaktperson/rådgivare för informationssäkerhetsfrågor, inkl. prefekter om det är formellt beslutat att de ska ha denna roll)	4	17
It-säkerhetschef	11	46
It-säkerhetsansvarig	19	79
It-arkitekt	17	71
Säkerhetschef	16	67
Säkerhetsskyddschef	13	54
Dataskyddsombud	24	100
Avtalsjurist(er) (forskningsavtal)	20	83
Avtalskoordinator(er) (forskningsavtal)	8	33
Förvaltningsjurist(er)	21	87,5
Dataskyddsjurist(er)	14	58
Ansvarig/samordnare för exportkontroll och produkter med dubbla användningsområden (PDA)	10	42
Data Access Unit (DAU)/forskningsdatateam eller motsvarande	22	92
Data steward eller motsvarande	5	21
Digitaliseringsansvarig	10	42
Arbetsgrupp för informationssäkerhet/motsvarande. Vänligen ange tjänstebefattning för de som deltar:	19	79
Andra för informationssäkerhetsarbetet relevanta roller, ange:	15	62,5
Om samma person har flera roller, vänligen beskriv vilka roller som innehas av samma person:	10	42

Fråga 4. Var i organisationen är informationssäkerhetschefen placerad?

Om den rollen inte finns, var är centralt anställd informationssäkerhetsspecialist/ informationssäkerhetssamordnare/informationssäkerhetsstrateg eller motsvarande placerad?

Antal svar: 21, valda alternativ: 25

	Antal	Procent
Rektors kansli/motsvarande	3	14
Förvaltningschefs stab/motsvarande	5	24
Annan avdelning/motsvarande på förvaltningen, ange:	5	24
It-avdelningen	10	48
Annat, ange:	2	9,5

Fråga 5. Sker reglerad rapportering från informationssäkerhetschefen till följande? Flera alternativ kan anges.

Om den rollen inte finns avses centralt anställd informationssäkerhetsspecialist/ informationssäkerhetssamordnare/informationssäkerhetsstrateg eller motsvarande. Med ”reglerad rapportering” avses här att det finns en formaliserad rutin för hur rapporteringen ska ske och att rapporteringen är regelbundet återkommande.

Antal svar: 21, valda alternativ: 58

	Antal	Procent
Lärosätets styrelse	8	38
Rektor	10	48
Förvaltningschef	11	52
Säkerhetschef	7	33
Säkerhetsskyddschef	3	14
It-chef	7	33
Annan, ange:	8	38
Ingen reglerad rapportering sker	4	19
Vet inte	0	0

Fråga 6. Diskuterades informationssäkerhet på lärosätets styrelsemöten under 2022?

Antal svar: 24

	Antal	Procent
Ja, på samtliga möten	3	12,5
Ja, men bara om något särskilt skulle rapporteras	15	62,5
Nej, det diskuterades inte	4	17
Vet inte	2	8

Fråga 7. Vänligen markera samtliga av följande dokument som är upprättade på lärosätet.

Markera även de styrdokument som finns på lärosätet som har andra namn än de nedan men som ni bedömer är motsvarande i innehåll.

Antal svar: 24, valda alternativ: 166

	Antal	Procent
Informationssäkerhetspolicy	24	100
It-säkerhetspolicy	8	33
Säkerhetspolicy	15	62,5
Policy för hantering av forskningsdata	12	50
Policy/riktlinje för forskningsavtal	3	12,5
Policy/riktlinje för exportkontroll	10	42
Policy/riktlinje för personuppgiftsbehandling	20	83
Riktlinje/anvisning för riskanalys och riskbedömning inom informationssäkerhet	17	72
Regler för bevarande och gallring av forskningshandlingar	23	96
Informationshanteringsplan	17	71
Andra dokument av relevans för informationssäkerhet, ange:	18	75

Fråga 8. När upprättades informationssäkerhetspolicyn och när reviderades den senast?

Antal svar: 23, valda alternativ: 43

	Antal	Procent
Upprättades*, ange datum	23	100
Vet inte när den upprättades	0	0
Reviderades**, ange datum:	13	56,5
Vet inte när den reviderades	0	0
Den har inte reviderats	7	30

*** Upprättades**

År	Antal
2007	2
2010	1
2013	2
2014	2
2017	4
2018	4
2019	2
2020	1
2021	3
2022	2

****Reviderades**

År	Antal
2014	1
2021	4
2022	4
2023	2
Pågående	2

Fråga 9. Kommentarer som rör avsnittet Roller och styrdokument

Antal svar: 13

Fråga 10. Har lärosätet gjort en inventering av de informationstillgångar som finns på lärosätet?

Med informationstillgångar avses här information som är relaterad till lärosätets verksamhet, med fokus på forskningsverksamheten. De inkluderar både informationen i sig och informationsbehandlade resurser (t.ex. programvara) som är av värde för organisationens verksamhet.

Antal svar: 24, valda alternativ: 24

	Antal	Procent
Ja, ange vad som inventerades:	15	62,5
Nej, ange varför:	7	29
Vet inte	2	8

Fråga 11. Har lärosätet en modell för informationsklassning?

Antal svar: 24, valda alternativ: 24

	Antal	Procent
Ja	21	87,5
Nej, ange varför:	3	12,5
Vet inte	0	0

Fråga 12. Vilka klassningsobjekt tillämpas modellen på?

Flera alternativ kan anges.

Antal svar: 21, valda alternativ: 68

	Antal	Procent
It-system och it-tjänster	17	81
Verksamhetsprocesser	6	29
Informationsmängder (Med ”informationsmängder” avses här en gruppering av information, exempelvis i form av dokument, en databas eller liknande, som innehåller flera informationstyper.)	17	81
Informationstyper (Med ”informationstyper” avses här ett visst slag av information, t.ex. personuppgifter.)	15	71
Forskningsprojekt/motsvarande	11	52
Annat, ange:	2	9,5
Den tillämpas inte, ange varför:	0	0

Fråga 13. Finns det en vägledning för hur informationsklassningen praktiskt kan genomföras, t.ex. med stöd och mallar?

Antal svar: 21

	Antal	Procent
Ja	18	86
Nej	3	14
Vet inte	0	0

Fråga 14. Kommentarer som rör avsnittet Identifiering av informationstillgångar och informationsklassning.

Antal svar: 11

Fråga 15. Gör lärosätet årligen en övergripande riskanalys på central nivå?

Med riskanalys avses den analys som görs i enlighet med förordningen (2007:603) om intern styrning och kontroll, eller motsvarande analys på ledningsnivå om förordningen inte är tillämplig på lärosätet.

Antal svar: 24

	Antal	Procent
Ja	21	87,5
Nej	2	8
Vet inte	1	4

Fråga 16. Har informationssäkerhet ingått i lärosätets årliga övergripande riskanalys?

Antal svar: 21

	Antal	Procent
Ja, fler än de senaste 5 åren i följd	7	33
Ja, de senaste 4 till 5 åren	3	14
Ja, de senaste 2 till 3 åren	6	29
Ja, i den senaste årliga riskanalysen	2	9,5
Ja, en eller flera av de senaste fem åren, men inte senaste året	1	5
Nej, har inte ingått något av de senaste fem åren	2	9,5
Vet inte	0	0

Fråga 17. Vilka av följande analyser har gjorts och dokumenterats i det lärosätesövergripande informationssäkerhetsarbetet?

Den riskanalys som avses här är den som bör göras enligt ISO/IEC 27000-serien. Se även MSB:s metodstöd för informationssäkerhet för vidare information.

Antal svar: 24, valda alternativ: 48

	Antal	Procent
Verksamhetsanalys, gjordes senast, ange år:	11	46
Omvärldsanalys, gjordes senast, ange år:	8	33
Riskanalys, gjordes senast, ange år:	15	62,5
Gapanalys, gjordes senast, ange år:	10	42
Ingen av ovanstående	3	12,5
Vet inte	1	4

Fråga 18. På vilka organisatoriska nivåer genomförs och dokumenteras en riskbedömning inom informationssäkerhet minst en gång per år? Flera nivåer kan anges.

Med riskbedömning avses en övergripande process som innefattar delprocesserna riskidentifiering, riskanalys och riskutvärdering (ISO/IEC 27000:2018).

Antal svar: 24, valda alternativ: 34

	Antal	Procent
Centralt/lärosätesövergripande	14	58
Alla fakulteter/motsvarande	4	17
Vissa fakulteter/motsvarande	1	4
Alla institutioner/motsvarande	6	25
Vissa institutioner/motsvarande	3	12,5
Inget av ovanstående	6	25
Vet inte	0	0

Fråga 19. Beskriv om forskningsdata ingår i riskbedömningen inom informationssäkerhet på någon av nivåerna.

Antal svar: 18

Fråga 20. Har lärosätet kartlagt vilka rättsliga krav och andra externa krav som påverkar hanteringen av forskningsdata vid lärosätet?

Andra externa krav kan t.ex. vara krav som finansiärer eller externa samverkanspartners ställer.

Antal svar: 24

	Antal	Procent
Ja	16	67
Nej	6	25
Vet inte	2	8

Fråga 21. Kommentarer som rör avsnittet Analys

Antal svar: 16

Fråga 22. Har lärosätet ett centralt incidentrapporteringssystem?

Antal svar: 24

	Antal	Procent
Ja, det inkluderar alla typer av incidenter	18	75
Ja, men det inkluderar inte informationssäkerhetsincidenter	3	12,5
Nej, det finns inte ett centralt incidentrapporteringssystem	3	12,5
Vet inte	0	0

Fråga 23. Har lärosätet interna rutiner för hur informationssäkerhetsincidenter ska...

Antal svar: 24, valda alternativ: 103

	Antal	Procent
identifieras	14	58
bedömas	14	58
hanteras	19	79
dokumenteras	19	79
rapporteras	17	71
följas upp	15	62,5
Vi har rutiner för hantering av incidenter, men de rör inte informationssäkerhetsincidenter	4	17
Inget av ovanstående	1	4

Fråga 24. Kommentarer som rör avsnittet Incidenter

Antal svar: 12

Fråga 25. Hur mycket personalresurser budgeterades 2023 för specifikt arbete med informationssäkerhet på central nivå på lärosätet?

Inkludera personal som i sin arbetsbeskrivning (eller motsvarande, exempelvis projekt- eller uppdragsbeskrivning) ska jobba med informationssäkerhet, it-säkerhet, dataskydd eller säkerhetsskydd. Inkludera även konsulter som har anlitats eller ska anlitas.

Antal svar: 24, valda alternativ: 31

	Antal	Procent
0 helårsarbetskrafter	0	0
Mer än 0 till mindre än 1 helårsarbetskrafter	1	4
1 till mindre än 2 helårsarbetskrafter	8	33
2 till mindre än 5 helårsarbetskrafter	10	42
Mer än 5 helårsarbetskrafter, ange hur många:	4	17
Vet inte	2	8
Om det finns vakanta tjänster kopplade till informationssäkerhetsarbetet, ange varför:	6	25

Fråga 26. Hur mycket finansiella resurser (SEK) budgeterades för informationssäkerhet på central nivå på lärosätet 2023?

Inkludera personalkostnader i form av löner inkl. konsulter, projektkostnader, kurser, utbildningar, seminarier och säkerhetsåtgärder (t.ex. en it-tjänst) vars primära syfte är att förbättra informationssäkerheten.

Antal svar: 24, valda alternativ: 24

	Antal	Procent
Ange i SEK:	11	46
Vet inte	13	54

Fråga 27. Om enskilda forskningsprojekt har identifierat behov av informationssäkerhetsåtgärder, hur finansieras vanligtvis dessa?

Du kan markera flera alternativ.

Informationssäkerhetsåtgärder kan vara både tekniska och administrativa.

Antal svar: 24, valda alternativ: 56

	Antal	Procent
Med medel från det enskilda forskningsprojektet där behovet uppstår	20	83
Med institutionsgemensamma medel	11	46
Med fakultetsgemensamma medel	5	21
Med universitetsgemensamma medel (t.ex. av central it-avdelning)	19	79
Annat, ange:	1	4
Vet inte	0	0

Fråga 28. Kommentarer som rör avsnittet Resurser till informationssäkerhetsarbete

Antal svar: 8

Fråga 29. Markera de externa och interna kurser och utbildningar med koppling till informationssäkerhet som erbjuds medarbetare vid lärosätet (medarbetare kan även inkludera konsulter).

Avser även digitala utbildningar.

Antal svar: 24, valda alternativ: 100

	Antal	Procent
Informationssäkerhet	23	96
Dataskydd/GDPR	18	75
Säkerhetsskydd	6	25
Exportkontroll/PDA	3	12,5
Forskningsdatahantering	14	58
Etikprövning	12	50
Immaterialrätt	6	25
Sekretess/OSL	13	54
Inget av ovanstående	0	0,
Annat, ange:	5	21

Fråga 30. Hur stor andel av medarbetarna har gått utbildningar i informationssäkerhet?

Antal svar: 22

	Antal	Procent
Mer än 0 till mindre än 25 procent	11	50
25 till mindre än 50 procent	5	23
50 till mindre än 75 procent	1	5
75 till 100 procent	1	4,5
Vet inte	4	18

Fråga 31. Kommentarer som rör avsnittet Utbildning och kurser

Antal svar: 12

Fråga 32. Vad har prioriterats i lärosätets informationssäkerhetsarbete de senaste två åren?

Antal svar: 22

Fråga 33. Vad i lärosätets nuvarande informationssäkerhetsarbete bedömer ni som mest angeläget att förbättra?

Antal svar: 23

Fråga 34. Vilka är de största utmaningarna när det gäller att bedriva ett systematiskt informationssäkerhetsarbete vid lärosätet?

Antal svar: 22

Fråga 35. Vad i lärosätets informationssäkerhetsarbete tycker ni fungerar bra?

Antal svar: 22

Fråga 36. Övriga kommentarer (kan också röra enkäten i sin helhet)

Antal svar: 5

Del 2

Missiv

Svaren på frågorna i den här delen av enkäten kan omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och kan innehålla säkerhetsskyddsklassificerade uppgifter. Det är viktigt att lärosätet gör en sekretessbedömning och eventuell säkerhetsskyddsklassificering av sina svar, samt meddelar sin bedömning till Riksrevisionen (se mer i informationsrutan nedan).

Riksrevisionen rekommenderar att frågorna nedan besvaras av säkerhetschef i samråd med berörda medarbetare, t.ex. informationssäkerhetschef eller motsvarande.

Inrapportering till Riksrevisionen ska ske enligt bifogad instruktion. Riksrevisionen vidtar nödvändiga säkerhetsåtgärder för att skydda informationen som överförts. Är det någon särskild aspekt ni har frågor kring så kontakta oss gärna.

Rapportera enligt nedan

Kopiera över enkäten till ett krypterat USB-minne och besvara frågorna. Lägg USB-minnet i säkerhetspåse. Skicka med rekommenderad post så att vi har det tillhanda **senast den 8 maj** till:

Riksrevisionen
Att. Ludvig Stendahl
Box 6181
102 33 Stockholm

När ni skickat USB-minnet, vänligen meddela detta via mejl till: Ludvig Stendahl
Mejla lösenordet till det krypterade USB-minnet till: Ludvig Stendahl

Bedömer lärosätet att den information som lämnas som svar på frågorna nedan omfattas av sekretess? Om ja, ange något av följande i rutan nedan: (1) Uppgift som omfattas av sekretess enligt OSL och som rör Sveriges säkerhet. Ange lagrum och skyddsnivå; (2) Sekretessmarkering; sekretess enligt OSL (ange paragraf).

[Exempelvis OSL 18:8, OSL 18:13, säkerhetsskyddsklass begränsat hemlig]

_____
_____

1. **Vilket lärosäte företräder du?** _____

2. **Vilken funktion har du som besvarar enkäten?** _____

3. **Har lärosätet en samlad förteckning eller flera förteckningar över verksamheternas skyddsvärda[1] informationstillgångar?**

   ☐ Ja, inklusive alla skyddsvärda forskningsdata[2]

   ☐ Ja, inklusive vissa skyddsvärda forskningsdata

   ☐ Ja, men den/de inkluderar inte skyddsvärda forskningsdata

   ☐ Nej *(varför inte?)* _____

   ☐ Vet inte

4. *Om ja på fråga 3:*
   När upprättades och uppdaterades senast förteckningen över skyddsvärda informationstillgångar?

   Upprättades: _____

   Uppdaterades: _____

5. *Om "Ja, inklusive alla/vissa skyddsvärda forskningsdata" på fråga 3:*
   Beskriv hur lärosätet gått till väga för att kartlägga vilka forskningsdata som är skyddsvärda.

   _____

6. **Har lärosätet genomfört en inledande verksamhetsanalys för att identifiera eventuell säkerhetskänslig verksamhet?**

   ☐ Ja *(ange år)* _____

   ☐ Nej *(varför inte?)* _____

   ☐ Vi genomför en just nu (våren 2023)

   ☐ Vet inte

[1] Med skyddsvärda avses här det som lärosätet själv anser ha ett förhöjt skyddsvärde i relation till lärosätets övriga information.

[2] Forskningsdata avser data som samlas in eller framställs inom ramen för vetenskaplig forskningsverksamhet. Det kan t.ex. vara digitala texter, bilder, audiovisuella material, 3D-skanningar, observationsdata, resultat från experiment och andra typer av digitala objekt. Sammanfattningsvis utgörs forskningsdata av det underlag som lett fram till ett forskningsresultat.

7. Har lärosätet genomfört en säkerhetsskyddsanalys?

☐ Ja *(ange år)* _____

☐ Nej *(varför inte?)* _____

☐ Vi genomför en just nu (våren 2023)

☐ Vet inte

☐ Ej tillämpbart (lärosätet har bedömt att det inte behöver göras)

Kommentar: _____

8. *Om ja på fråga 7:*
Har lärosätet en beslutad säkerhetsskyddsplan?

☐ Ja *(ange år)* _____

☐ Nej *(varför inte?)* _____

☐ Vet inte

9. Bedömer ni att ert lärosäte...

	Ja	**Nej**	**Vet inte**
...hanterar säkerhetsskyddsklassade uppgifter?	☐	☐	☐
...bedriver verksamhet som i övrigt behöver ett säkerhetsskydd?	☐	☐	☐
...bedriver verksamhet som omfattas av ett för Sverige förpliktigande åtagande om säkerhetsskydd?	☐	☐	☐

Tack för er medverkan!