

Ifølge liste

Deres ref

Vår ref

Dato

17/1224-

7. januar 2019

Kunnskapsdepartementets styringsmodell for informasjonssikkerhet i høyere utdanning og forskning

Digitalisering av høyere utdanning og forskning er en av mine hovedprioriteringer som forsknings- og høyere utdanningsminister. Digitalisering gir store muligheter for vårt samfunnsoppdrag, men fører også med seg nye trusler og sårbarheter. Det håndteres stadig større mengder verdifull informasjon i høyere utdanning og forskning, men mange virksomheter har utfordringer med internkontroll og styring av informasjonssikkerhet. Informasjonssikkerhet er en grunnleggende forutsetning for å kunne lykkes med digitalisering. Jeg vil derfor her informere om at Kunnskapsdepartementet innfører en ny modell for styring av informasjonssikkerhet og personvern i høyere utdanning og forskning. Samtidig forventer jeg at virksomhetene selv styrker egen styring av informasjonssikkerhet og personvern for å håndtere den risikoen økt digitalisering medfører¹.

Styret har det øverste ansvaret for risikoen som knytter seg til virksomhetens informasjonsverdier, og er ansvarlig for at sikkerheten er tilpasset denne risikoen. Det er styrets ansvar å sette virksomheten i stand til å håndtere risikoen slik at denne er på et nivå som styret aksepterer. Jeg forventer også at håndteringen av dette viktige området integreres i den generelle virksomhetsstyringen og er tydelig forankret i styret og toppledelsen.

Informasjonssikkerhet er en kritisk suksessfaktor for kunnskapsvirksomheter

Regjeringen lanserte i 2017 digitaliseringsstrategien for høyere utdanning og forskning. Direktoratet for IKT og fellestjenester i høyere utdanning og forskning (Unit) har i oppgave å

¹ Se f.eks. NSMs rapport *Et sikkert digitalt Norge – IKT-risikobilde 2018*, tilgjengelig på https://nsm.stat.no/globalassets/rapporter/nsm_ikt-risikobilde_2018_web.pdf

følge opp strategien. I strategien legges det vekt på at universiteter og høyskoler har et selvstendig og bevisst forhold til informasjonssikkerhet, herunder personvern, som en kritisk suksessfaktor for egne digitaliseringsstrategier og strategiske satsinger. Dette er spesielt viktig i kunnskapsvirksomheter hvor forvaltning og foredling av store mengder informasjon og data er en så viktig del av selve kjernevirksomheten. Det er derfor avgjørende at vi klarer å ivareta informasjon og data på en god måte og til beste for samfunnet. Dette er noe alle virksomheter innenfor høyere utdanning og forskning har et selvstendig ansvar for, og noen av resultatene vi skal oppnå er:

Vi skal hindre at uvedkommende får tilgang til konfidensiell informasjon, enten det er sensitive personopplysninger og forretningshemmeligheter i forskningen eller informasjon om studenter og ansatte ved universiteter og høyskoler. Vi skal sikre at informasjon er uforfalsket og til å stole på, enten det er rådata eller publisert informasjon i forskningen, eller studentenes eksamensresultater. Vi skal sikre at våre tjenester er tilgjengelige for alle brukerne som er avhengige av disse, enten det er ved våre egne virksomheter, eller for brukere på tvers av sektorer, landegrenser og langs stadig mer sammensatte verdikjeder. Mens vi kopler bygg, infrastruktur og utstyr på nett i et stadig raskere tempo, skal dette skje på en trygg måte som ivaretar liv og helse.

Informasjonssikkerheten er ikke god nok

Vi har utfordringer med å lukke de avvikene som skal gi en tilfredsstillende sikkerhet i dag. Eksempler på dette er Riksrevisjonens kritikk av manglende informasjonssikkerhet i administrative systemer og forskningssystemer, samt oppslag i media om studentopplysninger på avveie. Dette viser at det er nødvendig å heve kvaliteten på informasjonssikkerhets- og personvernarbeidet i sektoren, også med tanke på at universiteter og høyskoler skal være i stand til å oppfylle skjerpede rettslige krav til sikker elektronisk informasjonsforvaltning og forsvarlig håndtering av personopplysninger.

Et løft av sikkerheten er nødvendig for å lykkes med digitaliseringen

Jeg ønsker at virksomheter innenfor høyere utdanning og forskning skal ha et spesielt fokus på informasjonssikkerhet og personvern i arbeidet med å videreutvikle en kvalitetskultur. I digitaliseringsstrategien har derfor Kunnskapsdepartementet oppfordret institusjonene til å løfte informasjonssikkerheten høyere enn de nasjonale minstekravene for å være i stand til å gjennomføre en strategisk satsing på digitalisering. Samtidig har departementet satt som mål å styrke egen styring av informasjonssikkerhet på sektornivå gjennom et tydeligere rammeverk for hvordan denne styringen skal foregå. Departementet har i samarbeid med Unit besluttet at styringen av informasjonssikkerhet og personvern på sektornivå skal baseres på standarden ISO/IEC 27014:2013². Departementet og Unit har tilpasset styringsmodellen i standarden til sektornivået i høyere utdanning og forskning, og viktige

² ISO/IEC 27014:2013: Information technology — Security techniques — Governance of information security. Dette er en standard på overordnet nivå som beskriver anbefalte konsepter, prinsipper og prosesser for styring av informasjonssikkerhet.

prinsipper i modellen er helhetlig risikostyring, mål- og resultatstyring og kontinuerlig forbedring.

Gjennomføring

Modellen omfatter de styringsoppgavene departementet og Unit har ansvar for, og systematiserer denne delen av styringsdialogen og oppfølgingen av sektoren. Den beskriver prosesser og ansvarsdeling mellom disse, og den er kompatibel med anerkjente rammeverk for eierstyring og selskapsledelse. Kunnskapsdepartementet har gitt Unit ansvaret for den løpende sektorstyringen av informasjonssikkerhet og virksomhetene vil merke dette gjennom:

- Tydeligere retning: Det vil bli utarbeidet en delstrategi for informasjonssikkerhet og personvern med klare målsettinger for sektoren og virksomhetene.
- Planmessig iverksetting: Det vil bli utarbeidet en handlingsplan som iverksetter delstrategien og en overordnet policy som gir retningslinjer og kommuniserer krav.
- Tettere oppfølging: Unit vil kartlegge graden av måloppnåelse på virksomhets- og sektornivå. Dette vil blant annet skje gjennom undersøkelser av virksomhetenes arbeid med informasjonssikkerhet og personvern, og ved at det utarbeides en årlig risikovurdering for sektoren.
- Riktigere prioriteringer: Resultatene fra Units undersøkelser i sektoren og de årlige risikovurderingene vil danne grunnlaget for nye målrettede tiltak.
- Tilpasset veiledning: Unit vil lage veiledninger for arbeidet med informasjonssikkerhet og personvern tilpasset høyere utdanning og forskning.

I etableringen av styringsmodellen skal også Unit vurdere hvordan behovet for veiledning og praktisk bistand, som tidligere ble levert av Uninetts sekretariat for informasjonssikkerhet, best kan dekkes. Unit er ikke satt opp til å yte denne bistanden i dag. Virksomhetene som omfattes av styringsmodellen er:

- Statlige universiteter og høyskoler
- Norges forskningsråd
- De nasjonale forskningsetiske komiteene
- NOKUT – Nasjonalt organ for kvalitet i utdanninga
- Diku – Direktoratet for internasjonalisering og kvalitetsutvikling i høyere utdanning
- Nupi – Norsk utenrikspolitisk institutt
- Unit – Direktoratet for IKT og fellestjenester i høyere utdanning og forskning
- Uninett AS
- Simula AS
- NSD AS
- UNIS AS

Eierstyringen av aksjeselskapene skal skje i tråd med statens prinsipper for eierstyring og selskapsledelse. Sektorstyringen av informasjonssikkerhet overfor aksjeselskapene skal skje innenfor rammene av disse prinsippene. Som eier har departementet de samme forventningene til nivået på informasjonssikkerheten i aksjeselskapene som i de underliggende virksomhetene men styringen vil være forskjellig.

Unit vil ta kontakt og foreslå tidspunkter for besøk hos virksomhetene for å informere mer om styringsmodellen.

Med hilsen


Iselin Nybø

Kopi
Riksrevisjonen

Adresseliste

| | | | |
|--|-------------------------------|------|------------|
| Arkitektur- og designhøgskolen i Oslo | Postboks 6768 St. Olavs plass | 0130 | OSLO |
| De nasjonale forskningsetiske komiteene | Kongens gate 14 | 0153 | OSLO |
| Direktoratet for internasjonalisering og kvalitetsutvikling i høyere utdanning | | | |
| Høgskolen i Innlandet | Postboks 400 | 2418 | ELVERUM |
| Høgskolen i Molde | Postboks 2110 | 6402 | MOLDE |
| vitenskapelig høgskole i logistikk | | | |
| Høgskolen i Østfold | | 1757 | HALDEN |
| Høgskulen i Volda | Postboks 500 | 6101 | VOLDA |
| Høgskulen på Vestlandet | Postboks 7030 | 5020 | BERGEN |
| Kunsthøgskolen i Oslo | Postboks 6853 St Olavsplass | 0130 | OSLO |
| Nasjonalt organ for kvalitet i utdanningen | Postboks 578 | 1327 | LYSAKER |
| Nord universitet | Postboks 1490 | 8049 | BODØ |
| Norges forskningsråd | Postboks 564 | 1327 | LYSAKER |
| Norges Handelshøyskole | Helleveien 30 | 5045 | BERGEN |
| Norges idrettshøgskole | Postboks 4014 Ullevål Stadion | 0806 | OSLO |
| Norges miljø- og biovitenskapelige universitet | Postboks 5003 | 1432 | ÅS |
| Norges musikkhøgskole | Postboks 5190 Majorstua | 0302 | OSLO |
| Norges teknisk-naturvitenskapelige universitet | | 7491 | TRONDHEIM |
| NSD - Norsk senter for forskningsdata AS | Harald Hårfagres gate 29 | 5007 | BERGEN |
| OsloMet storbyuniversitetet | | | |
| Samisk høgskole | Hánnoluohkká 45 | 9520 | KAUTOKEINO |
| Simula Research Laboratory AS | Postboks 134 | 1325 | LYSAKER |

| | | | |
|---|---------------------------|------|----------------|
| UNINETT AS | Postboks 4769 Sluppen | 7465 | TRONDHEIM |
| Unit - Direktoratet for IKT og fellestjenester i høyere utdanning og forskning | Pb. 5883 Majorstuen | 0308 | OSLO |
| Universitetet i Agder | Serviceboks 422 | 4604 | KRISTIANSAND S |
| Universitetet i Bergen | Postboks 7800 | 5020 | BERGEN |
| Universitetet i Oslo | Postboks 1072 Blindern | 0316 | OSLO |
| Universitetet i Stavanger | | 4036 | STAVANGER |
| Universitetet i Sørøst- Norge | Postboks 235 | 3603 | KONGSBERG |
| Universitetet i Tromsø – Norges arktiske universitet | | 9019 | TROMSØ |
| Universitetssenteret på Svalbard | Postboks 156 | 9170 | LONGYEARBYEN |