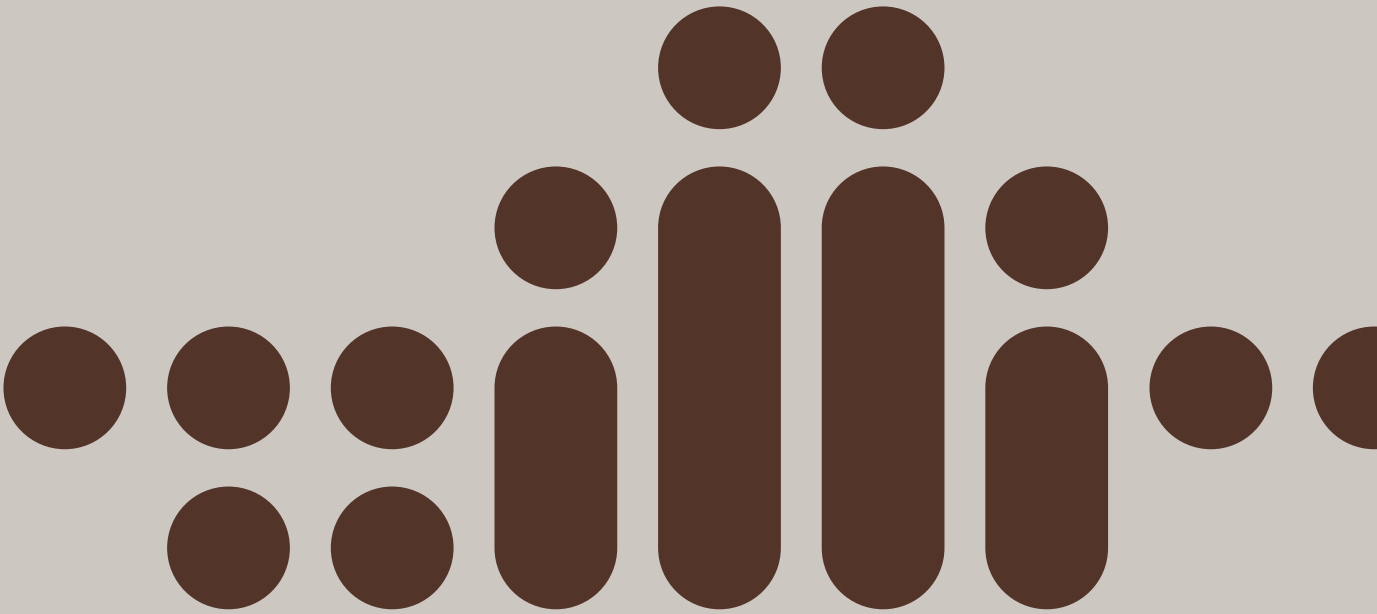
Kunnskapsdepartementet

April 2025

Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor



Innhold

Forord

Norge står overfor den mest alvorlige sikkerhetspolitiske situasjonen siden andre verdenskrig. Stormaktsrivalisering, økt terrorfare og den akselererende teknologiske utviklingen utfordrer sikkerheten vår. Kunnskapssektoren må være forberedt på å håndtere disse utfordringene over tid. Det krever mer av oss. Det krever økt beredskap.

I januar 2025 la regjeringen frem Totalberedskapsmeldingen. Meldingen setter kursen for hvordan den sivile motstandskraften vår skal styrkes. Vi skal være forberedt på krise og krig, motstå sammensatte trusler og være i stand til å understøtte militær innsats. Bak oss legger vi en tid hvor beredskap var basert på dyp fred. Fremover møter vi en farligere og mer uforutsigbar verden.

Kunnskapssektorens samfunnsoppdrag står helt sentralt i arbeidet med å styrke sivil motstandskraft. Kunnskap, kompetanse og teknologisk utvikling blir stadig viktigere for å bygge et robust samfunn og verne om våre grunnleggende verdier. Demokratiforståelse og kritisk tenkning er bærebjelker i norsk beredskap. Den enkelte virksomhets sikkerhet og beredskap må ivaretas for å kunne utføre samfunnsoppdraget. Et forsvarlig sikkerhetsnivå og egenberedskap er grunnlaget for å stå stødig i kriser og kunne bidra når det trengs. Det er dette arbeidet som styringsdokumentet retter seg mot.

Vi vet ikke hva den neste krisen vil være eller hvordan den vil foregå. Med styringsdokumentet ønsker vi å legge til rette for at virksomhetene jobber systematisk med sikkerhet og beredskap. Planlegging og oppfølging av grunnleggende tiltak reduserer risiko der det er mulig og gjør oss i stand til å møte det uforutsette bedre.

Styringsdokumentet samler alle kravene til departementets underliggende virksomheter og gir veiledning og anbefalinger til hele kunnskapssektoren. For å være et godt verktøy for både departementet og sektoren revideres dokumentet med jevne mellomrom. Til denne fjerde revisjonen har vi fått mange gode innspill fra ulike deler av sektoren. Det har styrket dokumentet.

Jeg er trygg på at dokumentet vil være til nytte og gjøre oss bedre forberedt, i den enkelte virksomhet, og i samhandlingen mellom virksomheter i sektoren.

Dag Thomas Gisholt
departementsråd

Oslo, 9. april 2025

1 Innledning

For å bidra til systematisk og god oppfølging av arbeidet med samfunnssikkerhet og beredskap i kunnskapssektoren, utviklet Kunnskapsdepartementet (KD) i 2011 et overordnet styringsdokument for dette arbeidet. Dokumentet har siden blitt revidert flere ganger, for å reflektere trussel- og risikobildet og nye krav og anbefalinger til arbeidet med sikkerhet og beredskap samt strukturelle endringer innenfor kunnskapssektoren. Dokumentet omhandler de tre sikkerhetsdomenene samfunnssikkerhet, statssikkerhet/nasjonal sikkerhet og informasjonssikkerhet. Det foreligger ulike krav og anbefalinger for hvert av disse domenene, og det kan være ulike fagmiljøer som jobber med dem. Derfor velger vi å opprettholde tidligere inndeling av «kravs- og forventningskapitlene» slik at kapittel 4 omhandler samfunnssikkerhet, kapittel 5 omhandler nasjonal sikkerhet og kapittel 6 omhandler informasjonssikkerhet. Samtidig er sammenhengene og overlappen mellom disse domenene tydeligere enn tidligere, noe som blant annet drøftes i avsnitt 2.2.

I tidligere utgaver av dokumentet har vi anbefalt å holde arbeidet med samfunnssikkerhet, nasjonal sikkerhet og informasjonssikkerhet separat fra helse, miljø og sikkerhet (HMS). Dette følger av at disse domenene har et annet sannsynlighets- og konsekvenspotensial enn HMS, ved i hovedsak å omhandle hendelser med lav sannsynlighet og potensielt høy konsekvens. Når det gjelder sikkerhet på virksomhetsnivå, ser vi imidlertid at det kan være krevende og uhensiktsmessig å skille HMS fra det øvrige sikkerhetsarbeidet. Det må derfor være opp til den enkelte virksomhet å vurdere hvordan de tre sikkerhetsdomenene og HMS integreres og/eller holdes adskilt.

Samfunnssikkerhetsinstruksen[1] understreker departementenes ansvar for samfunnssikkerhet i egen sektor og forklarer at «sektor» i denne sammenheng er departementets samlede politikkområde. Målgruppen for styringsdokumentet er dermed både departementets underliggende virksomheter og aktører som departementet har mer begrensede eller indirekte styringsmuligheter overfor, som kommunale og private virksomheter og forskningsinstitutter.

Styringsdokumentets relevans og bruk varierer i ulike deler av målgruppen. Flere av kravene som stilles til underliggende virksomheter vil for resten av sektoren være sterke anbefalinger. Der dette er aktuelt, står det tydelig at «KDs underliggende virksomheter skal / andre virksomheter i sektoren bør».

Dokumentet må sees i sammenheng med andre styringsdokumenter i sektoren, herunder instrukser, policyer og tildelingsbrev til departementets underliggende virksomheter, og den årlige budsjettproposisjonen (Prop. 1 S).

I dette dokumentet stilles det en rekke krav til KDs underliggende virksomheter (anbefalinger til de som ikke er underlagt KD). Noen av disse følger av departementets instruksjonsmyndighet. Dette gjelder spesielt innenfor samfunnssikkerhetsdomenet. Andre krav som stilles følger direkte av lover og forskrifter. Dette gjelder i hovedsak innenfor nasjonal sikkerhet og informasjonssikkerhet. Kravene (anbefalinger til de som ikke er underlagt) oppsummeres i blå bokser i kapitlene 4, 5 og 6.

[1] Justis- og beredskapsdepartementet (2017): *Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen)*.

2 Begreper og sammenhenger i sikkerhets- og beredskaps-arbeidet

2.1 Begrepsdefinisjoner

Nedenfor defineres begreper som er mye brukt i dokumentet. Definisjonene er i stor grad hentet fra Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden*.

Sektor er innenfor sikkerhetsarbeidet å forstå som et departements samlede politikkområde. Det omfatter områder som kan styres direkte av departementet, og som ivaretas av underlagte etater og virksomheter, samt de områdene hvor styringsmulighetene er mer begrensede. Sistnevnte er for eksempel områder som ivaretas av kommuner og private virksomheter.[2] Se ellers kapittel 3 om hvordan kunnskapssektoren er definert og KDs sektoransvar for sikkerhet og beredskap.

Samfunnssikkerhet er samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være utslag av tekniske eller menneskelige feil eller bevisste handlinger. Justis- og beredskapsdepartementet (JD) bruker begrepene «samfunnssikkerhetsfeltet» og «samfunnssikkerhetsarbeidet» når samfunnssikkerhet omtales i sin helhet eller overordnet. Samfunnssikkerhetsarbeid omfatter forebygging, beredskap og krisehåndtering. KD benytter samme terminologi som JD. Arbeidsmiljørelatert HMS-arbeid er i utgangspunktet ikke en del av samfunnssikkerhetsarbeidet, men det er viktig å se områdene i sammenheng.

Statssikkerhet er ivaretagelse av statens eksistens, suverenitet, territorielle integritet og politiske handlefrihet. Statssikkerhet har tradisjonelt vært knyttet til forsvaret av territoriet mot væpnede angrep, men den kan også utfordres ved påvirkning med ulike former for pressmidler mot norske myndigheter og samfunnsaktører.

Nasjonal sikkerhet er definert som statssikkerhet pluss den delen av samfunnssikkerhetsområdet, som er av vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser, ref. sikkerhetsloven punkt 1, § 1-3. bokstav e.

Informasjonssikkerhet handler om å beskytte informasjonsverdiers konfidensialitet, integritet og tilgjengelighet, uavhengig av informasjonens karakter og lagringsmedium, gjennom en risikostyringsprosess.[3]

Personopplysningssikkerhet inngår i arbeidet med informasjonssikkerhet, og handler om å beskytte personopplysninger mot utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført,

[2] Kommentardelen til samfunnssikkerhetsinstruksen, punkt 2, kapittel IV.

[3] Se for eksempel NS-ISO/IEC 27000 og NS-EN ISO/IEC 27001:2023.

lagret eller på annen måte behandlet.[4] Dette inkluderer tiltak for å sikre konfidensialitet, integritet og tilgjengelighet, og inngår som en del av den overordnede informasjonssikkerheten. I dette dokumentet brukes derfor i hovedsak begrepet informasjonssikkerhet, unntaket er der personopplysninger er særskilt omtalt.

Personvern kan forstås som vern av den personlige integriteten i utvidet forstand. Et vesentlig element i personvernet er at den enkelte skal ha kontroll over, og i størst mulig grad kunne bestemme over, egne personopplysninger. Dette innebærer en rett til å få vite hvilke opplysninger andre kjenner til om en selv og hva opplysningene brukes til. Dette omtales ofte som personopplysningsvern, og det er primært denne dimensjonen som er underlagt omfattende lovregulering gjennom blant annet personopplysningsloven, og regler om taushetsplikt.[5] Personvern er en rettighet som blant annet er nedfelt i Grunnloven og Den europeiske menneskerettskonvensjonen (EMK), og som strekker seg utover kun beskyttelse av personopplysninger.[6]

Nasjonale sikkerhetsinteresser er i sikkerhetsloven definert som landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til; (a) de øverste statsorganers virksomhet, sikkerhet og handlefrihet, (b) forsvar, sikkerhet og beredskap, (c) forholdet til andre stater og internasjonale organisasjoner, (d) økonomisk stabilitet og handlefrihet, og (e) samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet.[7]

Forebyggende sikkerhet benyttes i sikkerhetsloven og omfatter både tiltak som reduserer sannsynligheten for at en hendelse inntreffer og tiltak som reduserer virkningene ved en slik hendelse. *Forebyggende sikkerhetsarbeid* er planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende tiltak mot sikkerhetstruende virksomhet og følger av slik virksomhet.[8]

En krise er en uønsket situasjon med høy grad av usikkerhet og potensielt uakseptable konsekvenser for de enkeltpersoner, organisasjoner eller stater som rammes.

Sammensatte trusler er situasjoner der en aktør bruker et spekter av virkemidler for å påvirke oss. Begrepet brukes om strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt som kan kombinere diplomatiske, informasjonsmessige, militære, økonomiske, finansielle, etterretningsmessige og juridiske virkemidler for å nå strategiske målsettinger.[9] Virkemidlene kan brukes hver for seg eller settes sammen og koordineres slik at de understøtter og forsterker hverandre. De kan også brukes over en lang tidsperiode. Norske borgere, politikere og offentlige og private virksomheter kan være utsatt for slik virkemiddelbruk.

---

4 https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvik/hva-er-et-brudd-pa-personopplysningssikkerheten/

5 NOU 2022: 11 Ditt personvern -vårt felles ansvar. Tid for en personvernpolitikk.

6 Datatilsynet: Hva er personvern? (hentet 05.02.2025) og Store norske leksikon: personvern (hentet 05.02.2025)

7 Sikkerhetsloven § 1-5, punkt 1.

8 Sikkerhetsloven § 1-5, punkt 3.

9 Forsvarskommisjonen NOU 2023: 14 Forsvarskommisjonen NOU 2023: 14 *Forsvarskommisjonen av 2021 Forsvar for fred og frihet* s. 358.

Totalforsvar er en fellesbetegnelse for det militære forsvaret og den sivile beredskapen. Begrepet innbefatter den gjensidige støtten og samarbeidet mellom Forsvaret og det sivile samfunnet om forebygging, beredskapsplanlegging og operative forhold i fred, krise og krig.

Totalberedskap er samfunnets evne til, på en planmessig, forberedt og koordinert måte, å mobilisere dets samlede ressurser for å stå best mulig rustet overfor et sammensatt risiko- og trusselbilde.

2.2 Sammenhenger mellom sikkerhetsdomenene

Definisjonen av samfunnssikkerhet i 2.1 viser til *grunnleggende verdier*. Med dette forstås Grunnloven, beskyttelse av befolkningen, demokratisk styreform, menneskerettigheter, rettssikkerhet og rikets selvstendighet.[10] Med *grunnleggende funksjoner* menes funksjoner som er nødvendige for å ivareta befolkningens og samfunnets grunnleggende behov, for eksempel tilgang på livsnødvendigheter som mat, vann og varme, og vern mot uønskede hendelser. Verdiene det er vist til over, overlapper til en viss grad med verdier som statssikkerheten skal ivareta, jf. definisjonen over, men der samfunnssikkerheten i størst grad er rettet inn mot befolkningen og de samfunnene de lever i, retter statssikkerhet seg i større grad mot de øverste statsorganene, territoriet og vår nasjonale suverenitet. Noen vil si at statssikkerheten er en del av samfunnssikkerheten, mens andre vil si at statssikkerheten hviler på samfunnssikkerheten. En synes å være enig i at den gjensidige avhengigheten mellom disse sikkerhetsdomenene øker.

Norsk sikkerhets- og forsvarspolitikk skal sikre statssikkerheten, og har tradisjonelt sett vært knyttet til forsvaret av territoriet mot væpnede angrep. Gjennom sammensatt virkemiddelbruk trues på den ene siden statssikkerheten av andre former for pressmidler enn militære, og på den andre siden kan andre aktører enn sentrale myndigheter bli truet.

Desinformasjon, påvirkningsoperasjoner, fordekte investeringer i strategisk næringsvirksomhet, forstyrrelser i forsyningskjeder, innsidere i kommersielle eller offentlige virksomheter, hyppigere digitale angrep og sabotasjeaksjoner er blitt en alminnelig del av trusselbildet. Tradisjonelt er fred, krise og krig betraktet som steg på en linje mot det stadig mer alvorlige.[11] Slike steg er i stadig større grad upresise størrelser for å forstå den nye sikkerhetssituasjonen. Overgangene mellom fred, krise og krig blir mindre tydelige.

Bruken av sammensatte trusler utfordrer det tradisjonelle skillet mellom statssikkerhet og samfunnssikkerhet. Aktiviteten pågår ofte over lang tid og omfatter både lovlige og ulovlige virkemidler. Aktiviteten foregår ofte fordekt ved bruk av mellomledd, og i økende grad bruker statlige aktører profittmotiverte kriminelle til å gjennomføre aksjoner. Videre kan aktiviteten være krevende å forstå, oppdage, håndtere og motvirke, og den treffer oss alle.

[10] Totalberedskapskommisjonen: NOU 2023: 17 *Nå er det alvor* s. 51.

[11] Totalberedskapskommisjonen: NOU 2023: 17 s. 40.

Både samfunnssikkerhet og statssikkerhet er kollektive goder og en offentlig oppgave, men dette må bygges i fellesskap av blant annet befolkningen og private og frivillige aktører. Kunnskapssektoren har en viktig rolle i dette arbeidet.

Samfunnssikkerhetsinstruksen slår fast at arbeidet med informasjonssikkerhet er en integrert del av arbeidet med samfunnssikkerhet.[12] Samtidig finner statssikkerhetshendelser ofte sted i den digitale sfæren. Informasjonssikkerhet er altså omfattet av de to øvrige domenene, men samtidig foreligger det en rekke krav og anbefalinger som gjelder særskilt for informasjonssikkerhet. Dette gjør at det ofte kan være hensiktsmessig å skille ut informasjonssikkerhet som et eget domene, slik vi gjør i dette dokumentet. I tidligere versjoner av dette dokumentet er begrepet «informasjonssikkerhet og personvern» brukt. «Personvern» har i tidligere versjoner blitt brukt synonymt med «personopplysningssikkerhet», noe flere har opplevd som forvirrende. I denne nye versjonen brukes derfor «informasjonssikkerhet» alene. Dette skyldes at dokumentet primært handler om krav og anbefalinger til sikkerhetsstyring, mens «personvern» er et begrep som gjerne benyttes til å beskrive rettigheter og plikter med et videre formål enn kun sikkerhetshensyn. Det er fremdeles anbefalt å se arbeidet med informasjonssikkerhet og personvern i sammenheng.

[12] Kapittel II i samfunnssikkerhetsinstruksen.

2.3 Systematisk arbeid med sikkerhet og beredskap

Arbeidet med sikkerhet og beredskap er en kontinuerlig prosess der forebygging, beredskap, håndtering, gjenoppretting og læring kan ses på som en sammenhengende kjede, jf. figur 1. Kjeden har vært kjent som «samfunnssikkerhetskjeden», men illustrerer også arbeidet med de øvrige sikkerhetsdomenene. I Totalberedskapsmeldingen er undertittelen til kjeden «Arbeidet med sikkerhet og beredskap». I alle leddene av kjeden er kunnskapsoppbygging og tilpasning til endringer i trussel-, risiko- og sårbarhetsbildet en integrert del av arbeidet. Kjeden illustrerer de ulike fasene i sikkerhets- og beredskapsarbeidet, men også at dette arbeidet krever kontinuerlig oppmerksomhet om forbedring.

Figur 1 Arbeidet med sikkerhet og beredskap – et kontinuerlig forbedringsarbeid[13]

[13] Denne versjonen av figuren er hentet fra Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen. Forberedt på kriser og krig.*

2.4 Kunnskapssektorens bidrag til totalforsvaret og totalberedskapen

På bakgrunn av den mest alvorlige sikkerhetspolitiske situasjonen Europa har opplevd siden andre verdenskrig kom regjeringen våren 2025 med en melding til Stortinget om totalberedskap. Totalberedskapsmeldingen setter kursen for arbeidet med totalforsvaret og det sivile samfunnets motstandskraft i situasjoner der det verst tenkelige skulle skje, og Norge igjen skulle oppleve væpnet konflikt eller krig.[14]

Regjeringen har satt tre hovedmål for arbeidet med å styrke det sivile samfunnets motstandskraft:

1. Et sivilt samfunn som er forberedt på krise og krig
2. Et sivilt samfunn som motstår sammensatte trusler
3. Et sivilt samfunn som understøtter militær innsats

Totalberedskapsmeldingen slår fast at kunnskapssektoren spiller en avgjørende rolle i arbeidet med å styrke sivil motstandskraft og totalforsvaret.[15] Herunder har sektoren flere viktige oppgaver som del av sitt samfunnsoppdrag. Blant disse er:

- Å satse på forskning og kunnskapsutvikling innen samfunnssikkerhet og beredskap. I Langtidsplanen for forskning og høyere utdanning 2023–2032 (Meld. St. 5 (2022–2023)), jf. Innst. 170 S (2022–2023)) vil Regjeringen styrke arbeidet med samfunnssikkerhet og beredskap gjennom forskning, innovasjon og utdanning.
- Å drive studier innen samfunnssikkerhet, i tillegg til andre relevante studieretninger, blant annet innen digital sikkerhet.
- Å legge til rette for bedre samordning av FoU-systemene på sivil og militær side gjennom å utvikle et helhetlig forskningssystem for åpen, skjermet og gradert forskning
- Læreplanverket i skolen som legger godt til rette for at elevene lærer om kritisk tenkning og demokrati og blir aktive samfunnsborgere.
- Å styrke motstandskraften mot desinformasjon. Kunnskapssektoren spiller en særskilt rolle i dette arbeidet og er samtidig særlig utsatt ved at barn og unge er påvirkelige og ofte baserer seg på sosiale medier som nyhetskanaler. Samtidig er tilliten til forskning under press, en tillit som er avgjørende for et velfungerende demokrati.[16]

Punktene over omhandler hvordan virksomhetene i kunnskapssektoren bidrar til sivil motstandskraft gjennom sitt samfunnsoppdrag. Virksomhetenes evne til å ivareta sin egen sikkerhet og beredskap en viktig forutsetning for dette. Herunder

[14] Meld. St. 9 (2024–2025): s. 11

[15] Meld. St. 9 (2024–2025): s. 87.

[16] Våren 2025 legger regjeringen fram en ny strategi for å styrke befolkningens motstandskraft mot desinformasjon.

ser vi at forsyningssikkerhet blir stadig viktigere, blant annet gjennom virksomhetenes egenberedskap og deres evne til å håndtere forstyrrelser i forsyningskjeder.

I Totalberedskapmeldingen pekes det på at alle har et ansvar for å styrke den sivile motstandskraften i samfunnet og at den enkelte virksomhet kan bidra blant annet gjennom å:

- Tenke gjennom hvordan virksomheten kan opprettholde produksjon av varer og tjenester ved alvorlige hendelser som rammer samfunnet eller virksomheten.
- Lage beredskapsplaner for ulike typer hendelser som kan ramme virksomheten og virksomhetens drift.
- Lage rutiner for kollegastøtte og praktisere dette ved hendelser.
- Gjennomføre øvelser som kan sette virksomheten under press eller ut av drift.
- Følge NSMs grunnprinsipper for IKT-sikkerhet.
- Gjennomføre opplæring i råd om digital sikkerhet.
- Gjennomføre opplæring i kildekritikk.
- Peke ut en beredskapsansvarlig i virksomheten.[17]

KD oppfordrer virksomhetene til å forholde seg til listen. Flere av punktene følges også opp i senere kapitler, og noen av dem faller inn under eksisterende krav.

2.5 Sikkerhetsledelse, organisering og kompetanse

Sikkerhetskultur i en virksomhet er summen av kunnskap, handlinger og holdninger til sikkerhet. Alle virksomheter har en sikkerhetskultur, og kvaliteten på denne kulturen påvirker evnen til å styre sikkerheten og håndtere uønskede hendelser. En god sikkerhetskultur kjennetegnes ved at sikkerhetstiltak ivaretas, sikkerhetstruende hendelser rapporteres og læring prioriteres. Det er et lederansvar å legge til rette for å følge opp utviklingen av virksomhetens sikkerhetskultur.

Lederansvaret innebærer å gi nødvendige rammebetingelser og strukturer for sikkerhets- og beredskapsarbeidet. Det innebærer også ansvaret for å motivere medarbeidere til å handle på måter som ivaretar sikkerhet og beredskap. Medarbeidere må vite hva som forventes av dem og forstå hvorfor sikkerhetstiltakene eksisterer. Det krever opplæring, ansvarliggjøring og trygghet til å melde fra om sikkerhetstruende hendelser. For å lykkes med å lage en god sikkerhetskultur, må ledere gå foran som gode eksempler.

God sikkerhet og beredskap krever velfungerende samvirke på tvers av aktører og sektorer. En god sikkerhetskultur på virksomhets- og sektornivå innebærer da også respekt for hverandres roller og ansvar, samt forståelse for at ulike aktører har forskjellige oppgaver og perspektiver som må hensyntas og sees i sammenheng.

[17] Meld. St. 9 (2024–2025): s. 85.

Riktig kompetanse til å jobbe med sikkerhet og beredskap fordrer planmessig opplæring, kvalifisering og vedlikehold. § 7c i forskrift til sikkerhetsloven, virksomhetssikkerhetsforskriften, stiller krav til tilstrekkelig kompetanse om sikkerhet blant de som har tilgang til skjermingsverdige verdier.[18] Tilstrekkelig kompetanse er grunnleggende for alt arbeid med sikkerhet og beredskap.

[18] Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetssikkerhetsforskriften (VSF)) 2019.

3 Kunnskapsdepartementets ansvar for sikkerhet og beredskap

3.1 Hva menes med departementenes sektoransvar for sikkerhet og beredskap?

Når vi snakker om departementenes sektoransvar for sikkerhet og beredskap, er det gjerne samfunnssikkerhet det henspilles til. Dette fordi samfunnssikkerhetsinstruksen tydelig uttrykker at det enkelte departement har ansvar for samfunnssikkerhet, inkludert informasjonssikkerhet, i egen sektor. Departementenes «sektoransvar for samfunnssikkerhet» er et veletablert begrep. KD definerer imidlertid sektoransvaret for sikkerhet bredere, ved også å følge opp sektorens rolle og arbeid i lys av nasjonal sikkerhet og informasjonssikkerhet.

Ny sikkerhetslov trådte i kraft i 2019, og mange virksomheter i KDs sektor er omfattet av denne. Dette gjelder alle de offentlige virksomhetene. Lovens § 2-1 fastslår at departementene er ansvarlig for forebyggende sikkerhetsarbeid innenfor sitt ansvarsområde. Oppgavene for departementene er videre ikke så konkret beskrevet som i samfunnssikkerhetsinstruksen, men regelverket er tuftet på grunnleggende prinsipper for risikostyring i tråd med de som ligger til grunn for samfunnssikkerhetsinstruksen.

Sektoransvaret innebærer et ansvar for arbeid med forebygging, beredskap og krisehåndtering. Ansvaret er av overordnet art, samtidig skal departementene vurdere, beslutte og gjennomføre tiltak for å redusere sårbarhet innenfor hele politikkområdet, også der departementet ikke har direkte styringslinjer. Dette gjøres på bakgrunn av risikoanalyser. Samtidig har den enkelte virksomhet det operative ansvaret for å ivareta samfunnssikkerheten ved egen virksomhet. Det følger av ansvars- og nærhetsprinsippet.[19] I tilfellet skoler og barnehager følger det av forskrift om miljø og helse i skoler, barnehager og skolefritidsordninger at eier har ansvar for at kravene blir oppfylt jf. kap. 3 i veilederen til forskriften. Likevel følger det av ansvarsprinsippet at også den enkelte skole- og barnehageleder har et løpende ansvar.

Samfunnssikkerhetsinstruksen stiller krav til at arbeidet med samfunnssikkerhet skal være basert på et system for risikostyring, være preget av sammenheng og kontinuitet, og være kunnskaps- og erfaringsbasert. Hvert departement skal blant annet kunne dokumentere at det utarbeider og vedlikeholder systematiske ROS-analyser med grunnlag i vurderinger av hendelser som kan true departe-

[19] Ansvarsprinsippet innebærer at den organisasjon som har ansvar for et fagområde i en normalsituasjon, også har ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser på området. Nærhetsprinsippet innebærer at kriser skal organisatorisk håndteres på lavest mulig nivå.

mentets og sektorens funksjonsevne og sette lov, helse og materielle verdier i fare. På bakgrunn av ROS-analyser skal departementet vurdere, beslutte og gjennomføre tiltak slik at sårbarheter og svakheter blir redusert. Departementet skal være forberedt på å ivareta krisehåndtering ved hendelser i, eller med konsekvenser for, egen sektor.

Nærhetsprinsippet legges til grunn for krisehåndteringen i KDs sektor. Departementets kriseledelse foretar strategiske beslutninger og sørger for at berørte underliggende virksomheter får den støtten og de fullmaktene som trengs. Det forutsetter god situasjonsforståelse og tett dialog med berørte underliggende virksomheter. Det er derfor viktig at varslings- og rapporteringsmekanismer er etablert og øves. Se kap. 4.2 for mer om etablering av varslingsrutiner mellom virksomhetene og departementet.

For å kunne følge opp kravene i instruksen, må departementet avklare og beskrive departementets politikkområde når det gjelder samfunnssikkerhet. Det innebærer at roller, ansvarsområder og oppgaver som har betydning for å ivareta samfunnssikkerheten må beskrives. Styringsdokumentet bidrar til å oppfylle og dokumentere etterlevelsen av disse kravene.

KD har et omfattende ansvar innen samfunnssikkerheten. Sektoren omfatter store deler av befolkningen og består av et stort mangfold av virksomheter med ulike behov og krav til sikkerhet. KD har definert alle de statlige underliggende virksomhetene, hele barnehage- og opplæringssektoren uavhengig av eierskap, de private høyskolene, de private fagskolene, folkehøgskolene, studentsamskipnadene og statsaksjeselskapene innenfor sektoransvaret.

Obligatorisk tiårig grunnskole og høy dekningsgrad i barnehage og videregående opplæring gjør at en svært stor andel av årskullene mellom 1 og 19 år oppholder seg i barnehage eller skole mange timer daglig. Eiere og ledere av barnehager, grunnskoler, videregående skoler og lærebedrifter har et ansvar for at barn og unge er trygge der de er. Institusjonene som gir voksne grunnskoleopplæring har et tilsvarende ansvar for tryggheten til de voksne elevene. Universitetene og høyskolene har også ansvar for store grupper av studenter og ansatte. Dette handler både om personlig trygghet for liv og helse, og om ivaretagelse av barn og unges personvern i all behandling av personopplysninger. Universitetene, høyskolene og universitetsmuseene forvalter dessuten betydelige verdier, som blant annet forskningsdata, forskningsinfrastrukturer, samlinger og historiske bygninger.

Oppsummert har KD ansvaret for følgende områder:

- Barnehager
- Det 13-årige utdanningsløpet fra grunnskolen til og med videregående opplæring
- Folkehøgskoler
- Høyere utdanning og høyere yrkesfaglig utdanning (fagskoleutdanning)
- Utdanningsstøtte og bevilgninger til studentvelferd
- Kompetansepolitikken, livslang læring og grunn- og videregående opplæring for voksne
- Forskningspolitikken og samordning mellom departementene i utøvelsen av forskningspolitikken

Heterogeniteten i eierskap, styringslinjer, styringsvirkemidler og statlige tilknytningsformer fører til at hva som ligger i utøvelsen av sektoransvaret overfor ulike deler av sektoren varierer stort. Departementet kan instruere de underliggende virksomhetene i hvordan de skal jobbe med sikkerhet og beredskap. Overfor de øvrige delene av sektoren, har departementet i hovedsak pedagogiske virkemidler til rådighet. Departementet oppfordrer like fullt alle virksomheter i sektoren til å arbeide systematisk med sikkerhet og beredskap i tråd med anbefalingene i styringsdokumentet.

3.2 Sektoransvaret for departementets underliggende virksomheter

KDs underliggende virksomheter
KD har en rekke underliggende virksomheter av ulik størrelse, mandat og oppgaver og har et særskilt ansvar for sikkerheten og beredskapen ved disse virksomhetene. I styringen av sikkerhets- og beredskapsarbeidet ved de underliggende virksomhetene benytter KD instruksjonsmyndigheten og ulike andre virkemidler. Departementets styringsvirkemidler kan deles inn i følgende hovedgrupper (som i praksis ikke trenger å være klart atskilt fra hverandre): juridiske, økonomiske, organisatoriske og pedagogiske. Mer om hva departementet konkret krever av disse virksomhetene følger i kapitlene 4, 5, og 6.

De underliggende virksomhetene er:

- De statlige høyere utdanningsinstitusjonene
- 22. juli-senteret
- FEK – De nasjonale forskningsetiske komiteene
- HK-dir – Direktoratet for høyere utdanning og kompetanse
- FUB – Foreldreutvalget for barnehager
- FUG – Foreldreutvalget for grunnopplæringen
- Statens Lånekasse for utdanning
- NOKUT – Nasjonalt organ for kvalitet i utdanningen
- Norges forskningsråd
- NUPI – Norsk utenrikspolitisk institutt
- SIKT – Kunnskapssektorens tjenesteleverandør
- Statped
- Udir – Utdanningsdirektoratet
- VEA – Norges grønne fagskole

Fastsettelse av mål for arbeidet med sikkerhet og beredskap
I KDs budsjettproposisjon gis en omtale av sikkerhetsarbeidet innenfor alle sikkerhetsområdene, der det både rapporteres på spesielt viktige gjennomførte aktiviteter og tiltak og orienteres om mål og prioriteringer.

Styringsdokumentet er det viktigste virkemiddelet for å formidle krav som er konstante over en lengre tidsperiode. Ved revisjonen av styringsdokumentet i 2021 ble målsettinger og resultatoppfølging utvidet til det forebyggende sikkerhetsarbeidet innen nasjonal sikkerhet, og til informasjonssikkerhet.

Ordinær styringsdialog
KD følger opp sikkerhets- og beredskapsarbeidet blant annet gjennom tildelingsbrev, etatsstyringsmøter og brev med tilbakemelding i tilknytning til den årlige etatsstyringen og kontroller. Ved behov kan KD også ta initiativ til egne møter eller sende brev med tilbakemelding om behov for å iverksette tiltak. Virksomhetenes virksomhets- og økonomiinstrukser benyttes også for å understreke virksomhetenes ansvar på dette feltet. I tillegg er dette styringsdokumentet et sentralt virkemiddel i styringsdialogen rundt sikkerhet og beredskap. I noen tilfeller sendes egne brev med egne oppdrag, rapporteringskrav eller andre forventninger til virksomhetene.

Kontroll av arbeidet med sikkerhet og beredskap
For å etterleve sektoransvaret for arbeidet med sikkerhet og beredskap, er det viktig med en god situasjonsforståelse av sikkerhetstilstanden i sektoren. KD kartlegger og kontrollerer arbeidet med sikkerhet og beredskap på litt ulike måter innenfor henholdsvis høyere utdannings- og forskningssektoren på den ene siden, og barnehage- og skolesektoren på den andre siden.

For underliggende virksomheter i høyere utdannings- og forskningssektoren har HK-dir fått ansvaret for både å kartlegge og kontrollere sikkerhetsarbeidet på vegne av KD. Dette gjelder for arbeidet med samfunnssikkerhet, informasjonssikkerhet og personvern, og nasjonal sikkerhet. Resultatene fra kartleggingen og kontrollen er viktig for departementets situasjonsforståelse, og ligger til grunn for oppfølgingen av den enkelte virksomhets sikkerhets- og beredskapsarbeid. På bakgrunn av informasjonen som kommer frem av arbeidet, utarbeider HK-dir også forslag til sektortiltak innenfor alle sikkerhetsdomenene.

KD har selv ansvar for tilsvarende kontroll av underliggende virksomheter utenfor høyere utdannings- og forskningssektoren. Departementet gjennomgår rapporteringen om sikkerhet og beredskap i årsrapportene og tar ved behov opp avvik, mangelfull rapportering mv. med den enkelte virksomhet i den ordinære styringsdialogen.

Nasjonal sikkerhetsmyndighet (NSM) har ansvaret for at det i alle sektorer blir gjennomført kontroller av det forebyggende sikkerhetsarbeidet etter sikkerhetsloven. NSM skal videre se til at det føres tilsyn med at virksomheter oppfyller krav som følger av sikkerhetsloven med forskrifter. Departementet kan tildele en eksisterende sektormyndighet ansvar for å føre tilsyn med forebyggende sikkerhetsarbeid i sin sektor. KD har ikke foretatt en slik tildeling. Tilsynsmyndigheten innen forebyggende sikkerhetsarbeid i KDs sektor er derfor NSM. Formålet med tilsyn på dette området er å skape tillit til det forebyggende sikkerhetsarbeidet og bidra til å redusere sårbarheter i virksomhetene, i sektoren og nasjonalt.

3.3 Sektoransvaret for virksomheter som ikke er underlagt departementet

Nedenfor følger en gjennomgang av hvordan departementet kan benytte ulike virkemidler overfor de delene av sektoren som ikke er direkte underlagt departementet og som KD dermed ikke har instruksjonsmyndighet overfor. I tillegg kommer eierstyring av heleide aksjeselskaper og selskaper der departementet har dominerende eierinnflytelse.

Overfor alle disse virksomhetene er de pedagogiske virkemidlene, i form av veiledninger, møteplasser mv. viktige. Se Beredskapsrådet, udir.no og sikresiden.no for gode råd og veiledning, i tillegg til øvrige generiske ressurser i listen til slutt i dokumentet.

Barnehagesektoren
Barnehageeier har ansvar for at virksomheten drives i samsvar med gjeldende lover og regelverk. Kommunene eier i underkant av halvparten av barnehagene, og har dermed en rolle både som barnehageeier og barnehagemyndighet. Myndighetsoppgavene omfatter alle barnehagene i kommunen, både kommunale og ikke-kommunale, og innebærer blant annet å føre tilsyn med at barnehager drives i tråd med lov og regelverk.

Barnehagens arbeid med beredskap er regulert i forskrift om helse og miljø i barnehager, skoler og skolefritidsordninger som er en del av Helse- og omsorgsdeparte-

mentets (HODs) regelverk.[20] Forskriftens § 14 sier at virksomhetens sikkerhets- og beredskapsarbeid skal forebygge at ulykker skjer og begrense konsekvensene av uønskede hendelser så mye som mulig. Videre skal arbeidet med sikkerhet og beredskap integreres i barnehagens daglige drift. I rundskriv I-6/2015 er det presisert at barnehageeier (og skoleeier) ved leder av virksomheten også plikter å vurdere risiko for alvorlige tilsiktede hendelser, og planlegge beredskap ved virksomheten i henhold til dette risikobildet.

Kommunen fører tilsyn med barnehagenes oppfølging av forskriften. Statsforvalteren skal føre tilsyn med at kommunen utfører de oppgaver den er pålagt.

Grunnopplæringssektoren
Skoleeier har ansvar for at virksomheten drives i samsvar med gjeldende lover og regelverk. Kommunene eier de offentlige grunnskolene. Fylkeskommunene eier de offentlige videregående skolene, foruten de to samiske som er statlige, der KD har delegert etatsstyringsansvaret til Udir. Udir har status som skoleeier for de to samiske videregående skolene. I tillegg kommer private skoleeiere på begge skolenivåer.

Statsforvalteren veileder, fører tilsyn og behandler klagesaker etter opplæringsloven og friskoleloven. Se ellers avsnitt 3.4 om statsforvalteren.

Skolenes arbeid med beredskap er regulert i forskrift om helse og miljø i barnehager, skoler og skolefritidsordninger, jf. avsnittet om barnehagesektoren.

Tilsyn med skolenes oppfølging av forskriften føres av kommunen for grunnskoler og tilsvarende av fylkeskommunen for videregående skoler. Statsforvalteren skal føre tilsyn med at kommunen og fylkeskommunen utfører de oppgaver den er pålagt.

Høyere yrkesfaglig utdanning
De fleste fagskolene er enten private eller fylkeskommunale. Det er i dag fem statlige fagskoler, der to av disse ligger under KD, dykkerutdanningen som del av Høgskulen på Vestlandet, og Norges grønne fagskole (VEA). Vea er direkte underlagt KD, og følger dermed den samme styringslinjen som andre statlige utdanningsinstitusjoner. De fylkeskommunale fagskolene følger samme styringslinje som fylkeskommunale videregående skoler. Private fagskoler styres ikke utover de krav som følger av tilskuddsbrevene fra fylkeskommunene.

Fylkeskommunen fører tilsyn med de fylkeskommunale fagskolene og NOKUT med de private fagskolene.

Nasjonalt fagskoleråd har igangsatt et frivillig tiltak for å styrke arbeidet med samfunnssikkerhet og beredskap i fagskolesektoren. Rådet har som ambisjon å bidra til at statlige og private institusjoner opparbeider seg kunnskap om feltet slik at de kan arbeide systematisk og godt med dette.

Se ellers også avsnitt 7.1 om Beredskapsrådet, der fagskolene er representert.

[20] Forskrift om helse og miljø i barnehager, skoler og skolefritidsordninger.

Private høyskoler
For de private høyskolene foreligger ikke en direkte styringslinje fra KD, men det er en dialog med disse virksomhetene blant annet gjennom Beredskapsrådet. Departementet oppfordrer disse virksomhetene til å arbeide systematisk med sikkerhet og beredskap i tråd med anbefalingene i styringsdokumentet.

Se for øvrig også avsnitt 7.1 om Beredskapsrådet, der de private høyskolene er representert.

Studentsamskipnader
Studentsamskipnadene forvalter studentvelferden på vegne av staten. Ettersom samskipnadene er private særlovsselskaper, har ikke departementet direkte styring og stiller ikke krav i tilskuddsbrev til arbeidet med sikkerhet og beredskap. Departementet oppfordrer like fullt studentsamskipnadene til å arbeide systematisk med sikkerhet og beredskap i tråd med anbefalingene i styringsdokumentet.

Se ellers også avsnitt 7.1 om Beredskapsrådet, der studentsamskipnadene er representert.

Folkehøgskoler
Hovedandelen av folkehøgskolene har privat eierskap, mens noen få er fylkeskommunalt/kommunalt eide. Reguleringen i dagens folkehøgskolelov er ikke detaljert og gir få rettigheter og plikter. Dette har sammenheng med folkehøgskolenes særegenhet, at alle skolene skal ha elever i internat og at det gis opplæring uten krav om eksamen og sluttkompetanse.

Se ellers avsnitt 7.1 om Beredskapsrådet for UH-sektoren, der folkehøgskolene er representert.

Aksjeselskaper
Statsaksjeselskaper er aksjeselskaper der staten eier 100 prosent av aksjene. KD forvalter per 1. april 2025 det statlige eierskapet i to norske statsaksjeselskaper: Simula Research Laboratory AS og Universitetssenteret på Svalbard AS (UNIS). Både Simula og UNIS er konserner bestående av flere datterselskaper. I tillegg eier staten v/KD alle de norske aksjene i EISCAT AB, som er et svensk aksjeselskap eid av myndighetene i Sverige, Norge og Finland med 1/3 hver. I tillegg har de statlige universitetene og høyskolene eierskap, med varierende eierandeler, i en rekke aksjeselskaper.

Ansvaret for forvaltningen av aksjeselskaper ligger til styret til det enkelte selskap. Styret skal sørge for forsvarlig organisering av virksomheten og føre tilsyn med den daglige ledelsen og selskapets virksomhet for øvrig. Gjennom eierstyring i generalforsamlingen utøver departementet som aksjeeier den øverste myndighet i selskapet. Generalforsamlingen bør normalt ikke gripe inn i styrets forvaltning av selskapet. Rammene for eierstyring er ikke til hinder for at staten som eier tar opp forhold som selskapene bør vurdere i tilknytning til sin virksomhet og utvikling. De synspunkter staten gir uttrykk for i slike sammenhenger er å betrakte som innspill til selskapets administrasjon og styre. Styret har ansvar for å forvalte selskapet til beste for eierne og må foreta de konkrete avveininger og beslutninger.

Statsaksjeselskapene inngår i KDs sektoransvar for sikkerhet og beredskap, slik dette er definert tidligere i dokumentet. KDs heleide aksjeselskaper er blant annet underlagt de samme kravene som KDs underliggende virksomheter gjennom *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning*.[21] Når det gjelder de selskapene som universiteter og høyskoler har eierandeler i, vil også de kunne regnes som en del av sektoransvaret. Nivået på oppfølgingen fra departementets side må vurderes i det enkelte tilfellet, basert på flere ulike kriterier, blant annet risiko, vesentlighet, statens andel av eierskapet, hvor mye offentlig tilskudd de får, i hvilken grad de utøver oppgaver på vegne av staten og om aksjeselskapenes virksomhet omfatter ansvar for studenter og ansatte ved statlige institusjoner.

Forskningsinstituttene

KD har et overordnet politisk ansvar for forskningssikkerhet og et koordinerende ansvar for politikken overfor forskningsinstituttene. Forskningsinstituttene anses dermed som en målgruppe for anbefalingene i dette styringsdokumentet, selv om de enkelte instituttene eventuelt også er omfattet av sikkerhets- og beredskapsarbeid i sine respektive sektorer. Forskningsinstituttene utgjør en heterogen gruppe, både når det gjelder tilknytningsform og sektortilhørighet. I regjeringens Strategi for helhetlig instituttpolitikk fra 2020 blir regjeringens politikk overfor forskningsinstituttene avgrenset til tre grupper av institutter:

1. Forskningsinstitutter som får grunnbevilgning via Forskningsrådet (finansiert av NFD, KLD, LMD og KD)
2. Forskningsinstitutter som får driftsbevilgning direkte fra departementene (Havforskningsinstituttet (NFD), Statens arbeidsmiljøinstitutt (AID), Simula (KD), Forsvarets forskningsinstitutt (FD))
3. Offentlige institutter med FoU, men med annet hovedformål (Norsk polarinstitutt (KLD); Meteorologisk institutt (KLD); Nasjonalt folkehelseinstitutt (HOD); Norges geologiske undersøkelse (NFD); Norges vassdrags- og energidirektorat (ED); Arkivverket (KUD); Nasjonalbiblioteket (KUD); SSBs forskningsvirksomhet (FIN).)

KDs inkludering av forskningsinstituttene i arbeidet med forskningssikkerhet / sikkerhet i forskning, betyr i praksis at relevante institutter blir invitert til ulike møtearenaer og annen dialog som omhandler sikkerhet i forskningssektoren. Det betyr ikke at departementet tar ansvar for sikkerhets- og beredskapsarbeidet ved den enkelte institusjon. Som nevnt består instituttsektoren av institutter med ulik tilknytningsform. Noen er forvaltningsorganer, noen er stiftelser, noen aksjeselskaper. Det legges til grunn at institutter som er forvaltningsorganer, blir omfattet av sikkerhets- og beredskapsarbeidet til overordnet departement. For mer informasjon om forskningssikkerhet, se 5.6 om forskningssikkerhet og internasjonalt akademisk samarbeid.

[21] Rundskriv F-04-20 Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning. Policyen gjelder for alle statlige universiteter og høyskoler, HK-dir, NOKUT, Sikt, Norges forskningsråd, UNIS, Simula, De nasjonale forskningsetiske komiteer og NUPI.

Virksomhet i utlandet
Det er et betydelig antall norske borgere i utlandet som er i en opplæringssituasjon, arbeider med forskning eller er engasjert i annen aktivitet som er knyttet til KDs sektor. Utenriksdepartementet (UD) har hovedansvaret for å håndtere kriser i utlandet når nordmenn er rammet. UD gir råd og tips på sine landsider og utsteder offisielle reiseråd.

Ansvars- og nærhetsprinsippet tilsier at den enkelte virksomhet har ansvar for å etablere egne forebyggende tiltak og for beredskapsplanlegging som skal ivareta elevers og studenters sikkerhet i utlandet. Studenter i utlandet er en sammensatt gruppe som blant annet omfatter studenter på utvekslingsavtaler mellom norske og utenlandske universiteter og høyskoler. En annen gruppe er studenter som er på studiereise, og studenter/forskere på felt- eller praksisarbeid i utlandet i regi av en norsk høyere utdanningsinstitusjon. Disse inngår i KDs sektoransvar. Studenter som i egen regi studerer ved en utenlandsk institusjon faller ikke innunder dette ansvaret. For mer omtale av ansvaret for norske studenter i utlandet, se kap. 4. 10 i Meld. St. 7 (2020–2021) *En verden av muligheter – Internasjonal studentmobilitet i høyere utdanning*. Se ellers 5.1 om krise- og beredskapsplanverk der vi anbefaler at virksomheten vurderer å utarbeide planer for håndtering av hendelser som kan ramme studenter/forskere i utlandet, gjerne innlemmet i overordnet krise- og beredskapsplanverk.

3.4 Nasjonale myndigheters forhold til andre forvaltningsnivåer

Ansvaret for sikkerhet og beredskap på nasjonalt nivå ligger til departementene, men også statsforvalteren og kommunene har et stort ansvar, først og fremst for samfunnssikkerhet og beredskap, herunder for aktører i kunnskapssektoren.

Det er flere ulike styringslinjer som krysser hverandre i arbeidet med sikkerhet og beredskap i kunnskapssektoren. En styringslinje, ofte omtalt som «beredskapslinjen», går fra JD via Direktoratet for samfunnssikkerhet og beredskap (DSB) til statsforvalteren og videre til kommunen. KDs styringslinje for barnehage, grunnskole og videregående opplæring går via Udir til statsforvalteren og videre til kommunen og fylkeskommunen.

Statsforvalteren skal bidra til å styrke samfunnssikkerheten og krisehåndteringsevnen på regionalt og lokalt nivå.[22] Statsforvalteren skal utarbeide en ROS-analyse for fylket som skal legges til grunn for beredskapsplanleggingen, slik at forebyggende og beredskapsmessige tiltak gjenspeiler de risikoscenarioer som beskrives i ROS-analysen. Embetene skal ha en organisasjon som kan ivareta statsforvalterens oppgaver innenfor krisehåndtering.

Statsforvalteren har et særlig ansvar for tilsyn, oppfølging og veiledning av kommunene. Statsforvalteren må påse at kommunenes arbeid med samfunnssikkerhet

[22] Instruks for statsforvalteren og Sysselmesteren på Svalbard sitt arbeid med samfunnssikkerhet, beredskap og krisehåndtering.

og beredskap i tilstrekkelig grad omfatter barnehager, skoler og eventuelle andre utdanningsinstitusjoner som er lokalisert i den aktuelle kommunen.

Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven) trådte i kraft i 2010. Kravene til kommunene er spesifisert i lovens forskrift om kommunal beredskapsplikt fra 2011. Det kom ny veileder til forskrift om kommunal beredskap i april 2018. Formålet med kommunal beredskapsplikt er trygge og robuste lokalsamfunn. Dette oppnås gjennom systematisk og helhetlig samfunnssikkerhetsarbeid på tvers av sektorer i kommunen.

Forskriften stiller blant annet krav om at kommunene utarbeider helhetlige ROS-analyser for kommunen, beredskapsplaner og øvelser. Den helhetlige ROS-analysen danner grunnlag for kommunens langsiktige mål, strategier og tiltak i arbeidet med samfunnssikkerhet. Med utgangspunkt i ROS-analysen skal kommunen utarbeide en beredskapsplan med tiltak for å håndtere uønskede hendelser. Beredskapsplanen skal være oppdatert og revideres minimum én gang per år, og den skal øves jevnlig.

KD viser til lovbestemmelsene og forutsetter at kommunenes helhetlige ROS-analyser, beredskapsplaner og øvelser omfatter barnehager, skoler og eventuelle andre utdanningsinstitusjoner som er lokalisert i den aktuelle kommunen.

3.5 Særskilt om kritiske samfunnsfunksjoner og kritisk infrastruktur

Kritiske samfunnsfunksjoner er de funksjonene som er nødvendige for å ivareta befolkningens og samfunnets grunnleggende behov og befolkningens trygghetsfølelse. Med grunnleggende behov menes trygghet for den enkelte, og elementære fysiske behov som vann, mat, varme og lignende. De anleggene og systemene som er nødvendige for å opprettholde samfunnets kritiske funksjoner omtales som *kritisk infrastruktur*.

I oversikten i *Samfunnets kritiske funksjoner* er det definert 14 kritiske samfunnsfunksjoner og åtte hovedansvarlige departementer.[23] KD er ikke blant disse departementene, men er som alle andre departementer involvert i funksjonene «styring og kriseledelse» og «digital sikkerhet i sivil sektor». Virksomheter i sektoren er dessuten eiere av infrastruktur som bidrar til å opprettholde den samfunnskritiske funksjonen «digital sikkerhet i sivil sektor» (se avsnittet om kritisk infrastruktur nedenfor).

Årsaken til at virksomheter/tjenester i KDs sektor ikke er utpekt som kritisk samfunnsfunksjon er at dette som hovedregel forutsetter at et bortfall i opptil syv dager vil være kritisk for å ivareta befolkningens og samfunnets grunnleggende behov og trygghetsfølelse. Det er imidlertid verdt å nevne at KD, gjennom å være ansvarlig departement for barnehage og skole, er oppført som en *viktig samfunnsfunksjon* i Regjeringens midlertidige oversikt som ble opprettet i forbindelse med håndteringen av covid-19-pandemien.[24]

[23] DSB (2016): *Samfunnets kritiske funksjoner*.

[24] Regjeringen (2021): Liste over kritiske samfunnsfunksjoner, tilgjengelig på: https://www.regjeringen.no/contentassets/8da70b8196a24296ae730eaf99056c1b/liste-over-kritiske-samfunnsfunksjoner_oppdatert.pdf.

Kritisk infrastruktur i KDs sektor
KD definerer følgende systemer som kritisk infrastruktur i egen sektor:

1. **NIX (Norwegian Internet eXchange).** Dette er viktige samtrafikkpunkter for norsk internettrafikk som de fleste internettleverandører i Norge er tilkoblet, også private aktører som Telenor og andre internettilbydere. Hensikten med disse NIX-ene er å koble sammen deler av internettet i Norge. Disse samtrafikkpunktene driftes av USIT ved Universitetet i Oslo i samarbeid med fire andre universiteter (NIX-ene er plassert i Oslo, Bergen, Trondheim, Tromsø og Stavanger).
2. **Forskningsnettet.** Sikt – Kunnskapssektorens tjenesteleverandør utvikler og driver det norske forskningsnettet. Forskningsnettet forbinder mer enn 153 kunder og over 500 000 daglige sluttbrukere, og knytter dem opp mot internasjonale forskningsnett. Mange viktige tjenesteleverandører også utenfor universitets- og høyskolesektoren er avhengige av Forskningsnettet.
3. **Feide.** Dette er den nasjonale løsningen for sikker innlogging og datadeling i utdanning og forskning. Innloggingstjenesten skal både autentisere (bekrefte brukerens identitet) og autorisere brukeren (bekrefte status som elev/student/lærer, hvilke tjenester du *har* tilgang til og hvilke du *ikke* har tilgang til). Feide leveres av Sikt, og brukes både av høyere utdanning, grunnskolen, videregående skole og mange forskningsinstitusjoner. Løsningen har ca. 180 millioner årlige innlogginger.

Virksomheter som har ansvar for kritisk infrastruktur, må planlegge for å kunne opprettholde denne infrastrukturen. Som en viktig del av slik kontinuitetsplanlegging er det å kartlegge egen sårbarhet og iverksette tiltak for å redusere denne.

4 Krav og forventninger til virksomhetenes arbeid med samfunnssikkerhet

Tema	KDs underliggende virksomheter skal / andre virksomheter i sektoren bør:
Alle kravene skal dokumenteres skriftlig og dato for gjennomgang/revisjon må komme frem.	
ROS-analyse	• Utarbeide en helhetlig overordnet ROS-analyse. Analysen skal bygge på risikovurderinger fra nasjonal sikkerhet, informasjonssikkerhet og også se til HMS-feltet. • Gjennomgå analysen minimum hvert år og revidere den ved behov. • Presentere analysen i en helhetlig rapport. • Utarbeide en tiltaksplan til analysen for samtlige uønskede hendelser med middels eller høy risiko (denne kan inkluderes i den helhetlige ROS-rapporten). • I tiltaksplanen beskrive hvordan de enkelte tiltakene reduserer risikoen knyttet til den enkelte analyserte uønskede hendelsen.

Beredskaps-planverk	• Utarbeide en beredskapsplan. Gjennomgås årlig og revideres ved behov. Planen skal som et minimum inneholde:
	  • Definerte roller, oppgaver og fullmakter i en beredskapssituasjon eller krise
	  • Rutiner for krisekommunikasjon internt og eksternt
	  • Varslingsrutiner (herunder varsling av departementet)
	  • Varslingsrutiner (herunder varsling av departementet)
	• Utarbeide en kontinuitetsplan som del av beredskapsplanen. Holdes oppdatert og revideres ved behov.
	• Utarbeide en pandemiplan som utfyller beredskapsplanen. Revideres ved behov.

Beredskapsøvelser	• Utarbeide en årlig øvelsesplan som minimum skal inneholde:
	  • Formålet med den enkelte øvelse
	  • Tid og sted for gjennomføring
	  • Øvelsesscenario
	  • Type øvelse
	  • Målgruppe
	• Gjennomføre minimum en beredskapsøvelse per år. Øvelsene skal ta utgangspunkt i uønskede hendelser identifisert i virksomhetens ROS-analyse.

Evaluere øvelser og reelle hendelser	• Gjennomføre evalueringer i etterkant av hver beredskapsøvelse og etter reelle hendelser
	• Gjennomføre ledelsesforankrede oppfølgingsplaner med utgangspunkt i evalueringene. Disse skal som et minimum inneholde:
	  • Læringspunkter
	  • Beskrivelse av tiltakene
	  • Tidsramme/frist for gjennomføring av tiltakene
	  • Ansvarlig for hvert enkelt tiltak

4.1 Risiko- og sårbarhetsanalyser

KD forutsetter at alle aktører i sektoren jobber helhetlig og systematisk med sikkerhet og beredskap. Ved å legge risiko- og sårbarhetsanalyser (ROS-analyser) til grunn, legger man et godt grunnlag for å følge en risikobasert tilnærming til arbeidet med sikkerhet og beredskap.

Råd for samfunnssikkerhet og beredskap (Beredskapsrådet) har utarbeidet en veileder i risiko- og sårbarhetsanalyser for kunnskapssektoren. Veilederen er primært rettet mot virksomheter innen høyere utdanning og forskning, men den faglige tilnærmingen til ROS-analyseprosessen er også nyttig for andre virksomheter og sektorer. Dette avsnittet bygger på veilederen.

Veilederen retter seg mot overordnet ROS-analyse relatert til samfunnssikkerhet (heretter overordnet ROS-analyse). Denne analysen kobles til samfunnssikkerhet ettersom verdiene en gjennom analysen ønsker å beskytte, er menneskers liv og helse og opprettholdelse av driften av virksomheten.

I tråd med helhetsperspektivet, må en overordnet ROS-analyse relatert til samfunnssikkerhet se til tidligere utførte risikovurderinger (risikoanalyser) innenfor samfunnssikkerhet, nasjonal sikkerhet (jf. kap 5) og informasjonssikkerhet (jf. kap. 6) og vurdere hvilke uønskede hendelser som bør inkluderes i den overordnede analysen. Den overordnede ROS-analysen skal vektlegge de hendelsene som har et betydelig konsekvenspotensial med hensyn til menneskers liv og helse og opprettholdelse av driften. Det kan være at hendelser som er omfattet av tidligere utførte risikovurderinger på HMS-området også er relevante å ta med inn i en overordnet ROS-analyse.

Målet med ROS-analyser er å identifisere uønskede hendelser som kan inntreffe, vurdere risiko og sårbarhet knyttet til hendelsene på et overordnet nivå og gi et underlag for valg av tiltak for å redusere risiko og sårbarhet. Analysene kan også bidra til å styrke erkjennelsen av risiko i en virksomhet. Risikoerkjennelse er en forutsetning for å forebygge, redusere og håndtere risiko. Virksomhetens ledelse kan gjennom ROS-analysene både forstå risikoen de kan bli utsatt for og erkjenne ansvaret for å håndtere den. ROS-analysene ligger til grunn for det øvrige sikkerhets- og beredskapsarbeidet, som utviklingen av beredskapsplaner og planlegging av beredskapsøvelser.

Arbeidet med ROS-analyser er en systematisk prosess som kan baseres på ulike fremgangsmåter og standarder, deriblant ISO 31000:2018 (Risikostyring) og NS 5814:2021 (Risikovurderinger). Noe som går igjen er hoveddelene i selve prosessen: en planleggingsfase og forarbeid, en gjennomføringsfase, og en oppfølgingsfase. ROS-analyser må tilpasses virksomhetens størrelse og egenart. Det er stor variasjon innenfor KDs sektor, fra små barnehager og skoler til store universiteter og høyskoler, og fra opplæringsvirksomheter til rene forvaltningsorganer. Det er viktig at virksomhetene tar utgangspunkt i egen situasjon og tilpasser analysene til hva som er relevant for denne. ROS-analysene skal være nyttige verktøy i det konkrete arbeidet med sikkerhet og beredskap.[25]

[25] Beredskapsrådet (2022): Veileder i risiko- og sårbarhetsanalyser for kunnskapssektoren: s. 5-8.

De ulike trinnene i ROS-analysearbeidet skal dokumenteres i en helhetlig rapport. Det er videre viktig at ROS-analysen følges opp med konkrete tiltak overfor uønskede hendelser som vurderes til å inneha middels og høy risiko. Dette må synliggjøres gjennom utarbeidelse av en tiltaksplan. Tiltaksplanen skal beskrive hvordan de enkelte tiltakene reduserer sannsynligheten for, og konsekvensene av, uønskede hendelser.

En virksomhets ROS-analyse må minimum gjennomgås hvert år og revideres ved behov. Det er vesentlig at analysen gir mest mulig oppdatert informasjon om risiko og sårbarhet. Endringer i konteksten, som at virksomheten blir omorganisert eller får nye oppgaver, at verdiene virksomheten har definert som beskyttelsesverdige blir redefinert, eller trusselbildet endrer seg, kan være grunner til å revidere ROS-analysen.

Gjennomgang av ROS-analysen, og eventuell revisjon, skal kunne dokumenteres.

Om forholdet til trussel- og risikovurderinger for sektor og på nasjonalt nivå
KD anbefaler at virksomhetene i sitt arbeid med ROS-analyser henter inspirasjon fra blant annet DSBs krisescenarioer og de årlige trussel- og risikovurderingene fra henholdsvis NSM, Politiets sikkerhetstjeneste (PST) og E-tjenesten i identifiseringen av relevante hendelser for egen virksomhet. I DSBs krisescenarioer analyseres svært alvorlige hendelser samfunnet bør kunne forebygge og håndtere konsekvensene av. DSB tar utgangspunkt i større kriser som rammer samfunnet som helhet, og som derfor også kan ramme virksomheter i KDs sektor.

KD gjennomfører en helhetlig risiko- og sårbarhetsanalyse av sektoren (Sektor-ROS) med noen års mellomrom. Analysen tar utgangspunkt i overordnede nasjonale planleggingsgrunnlag som krisescenarioer, trussel- og risikovurderinger og bygger der det er naturlig på analyser og vurderinger gjort av underliggende virksomheter. ROS-analyser fra underliggende virksomheter og kommuner legges også til grunn. Analysen er unntatt offentlighet, men kan deles på anmodning.

4.2 Beredskapsplanverk

En krise kan oppstå som en plutselig hendelse, som en eskalerende hendelse som gradvis går fra normal håndtering til krisehåndtering, eller som en varslet krise. Krisesituasjoner krever ofte svært raske beslutninger og iverksettelse av tiltak på en raskere og mer effektiv måte enn i en normal situasjon. Det er derfor viktig å ha utarbeidet en krise- og beredskapsplan som raskt kan tas i bruk for å håndtere ulike typer kriser.

Alle virksomheter må utvikle og vedlikeholde beredskapsplaner for håndtering av uønskede hendelser eller kriser. Planen skal utarbeides på grunnlag av ROS-analysen.

Beredskapsplanen må være lett tilgjengelig, og må som et minimum inneholde:

- Organiseringen av beredskapsarbeidet med definerte roller, ansvar, oppgaver og fullmakter i en beredskapssituasjon eller krise.
- Rutiner for krisekommunikasjon internt og eksternt.
- Varslingsrutiner (avklare hvem som skal varsles og hvem som har ansvaret for dette, samt hvordan varsling skal finne sted).
- Kontinuitetsplan som del av beredskapsplanen. Holdes oppdatert og revideres ved behov.
- Pandemiplan som utfyller beredskapsplanen. Revideres ved behov.

Ved alvorlige hendelser skal virksomhetene varsle KD. En indikator på at det er en alvorlig hendelse er at man setter krisestab. Når og hvordan virksomhetene skal varsle departementet om alvorlige hendelser, skal inngå i virksomhetens etablerte varslingsrutiner, jf. tredje kulepunkt i listen over. Virksomhetene har ansvar for å holde departementet tilstrekkelig orientert ved en hendelse. I tillegg til varsling, innebærer dette også informasjonsdeling og rapportering. Informasjon om KDs beredskaps-epost og beredskapsnummer er kommunisert direkte til KDs underliggende virksomheter. Ved hastesaker skal man benytte telefonnummeret. Ta kontakt med KD dersom virksomheten ikke har tilgang på denne kontaktinformasjonen.

Virksomhetene skal som en del av beredskapsplanen utarbeide en kontinuitetsplan for å opprettholde kritiske funksjoner ved høyt personellfravær, uavhengig av årsak.

Pandemi vurderes som et høyst relevant scenario som kan ramme kunnskapssektoren hardt. Det må tas høyde for dette i den enkelte virksomhet ved å utarbeide en egen pandemiplan som utfyller beredskapsplanen. Virksomhetene kan i tillegg velge å utarbeide egne planer for håndtering av andre bestemte hendelser. Eller innlemme disse i beredskapsplanen, for eksempel som situasjonsspesifikke tiltakskort.

Virksomhetene må årlig gjennomgå beredskapsplanverket, og revidere ved behov. Dette er særlig aktuelt når virksomhetene oppdaterer sine ROS-analyser eller i etterkant av øvelser og reelle hendelser der krise- og/eller hendelseshåndteringsevnen til virksomheten er prøvd ut.

4.3 Beredskapsøvelser

Øvelser er læringsarenaer som skal bidra til at ledere og medarbeidere i virksomheten kjenner beredskapsplanen, sin rolle og sine oppgaver i en krisesituasjon. Det er en viktig forutsetning for å lykkes i håndteringen av uønskede hendelser og kriser.

Ved prioritering og valg av øvingsscenario skal virksomhetene ta utgangspunkt i ROS-analysen, herunder uønskede hendelser med høy eller middels risiko.

Øvelser kan ha ulik form, for eksempel: (1) diskusjonsøvelse hvor øvingsdeltakerne diskuterer ulike problemstillinger i tilknytning til et scenario, (2) spilløvelse, hvor det utføres handlinger mot en spillstab som fyller aktuelle roller, eller (3) fullskalaøvelse, som er den øvingsformen som ligner mest på en virkelig situasjon ved at man øver

mot reelle instanser. Hvilken form som er hensiktsmessig, avhenger av øvelsens hensikt og mål, samt tilgjengelige ressurser.

Samfunnssikkerhetsinstruksen stiller krav til at departementene evaluerer og følger opp hendelser og øvelser. Kravene er også relevante for virksomhetene i sektoren.

For de virksomhetene som er underlagt sikkerhetsloven, stiller virksomhetssikkerhetsforskriften krav til regelmessige øvelser for å kontrollere effekten av sikkerhetstiltakene i en normalsituasjon og av tiltakene som er planlagt ved økt trusselnivå.[26]

Øvelser må evalueres. Evalueringen må dokumenteres. Forbedrings- og læringspunkter som avdekkes i evalueringen må følges opp og konkretiseres i en oppfølgingsplan. Virksomhetene skal utarbeide en ledelsesforankret oppfølgingsplan. Som minimum skal den inneholde:

- Læringspunkter
- Konkret beskrivelse av tiltak
- Tidsramme/frist for gjennomføring av tiltak
- Ansvarlig for hvert enkelt tiltak

En øvelse er ikke ferdigstilt før samtlige punkter i oppfølgingsplanen er fulgt opp.

For å strukturere øvingsvirksomheten skal virksomhetene utarbeide en årlig øvingsplan. Som minimum skal den inneholde:

- Formålet med den enkelte øvelse
- Tid og sted for gjennomføring av øvelsene
- Øvelsesscenario
- Type øvelse
- Målgruppe

Øvingsplanen skal sørge for at virksomheten har en systematisk tilnærming til øvelser, hvor hele organisasjonen og samtlige aktuelle krisescenarioer øves over tid. Som et minimum skal det gjennomføres én øvelse hvert år. Det er ikke nødvendig at hele organisasjonen øves hver gang. Kriseledelsen må håndtere hendelsen for at det skal regnes som en krise- og beredskapsøvelse. Virksomhetene bør gjennomføre krise- og beredskapsøvelser sammen med eksterne aktører/samarbeidspartnere som kommunen, politiet og andre beredskapsetater, eller sammen med departementet.

DSB utarbeidet i 2016 en grunnbok og metodehefter for ulike typer øvelser, som kan være nyttige å benytte.

[26] Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetssikkerhetsforskriften) § 9.

4.4 Hendelser

På samme måte som med øvelser, må man gjennomføre en evaluering i etterkant av alvorlige hendelser. Når en hendelse er ferdig håndtert og man har fått gjenopprettet et akseptabelt sikkerhetsnivå, er det viktig at man så snart som mulig får evaluert hendelsen og håndteringen av denne, for å forhindre at fremtidige situasjoner oppstår og/eller reduserer konsekvensene.

Evaluering av hendelser må dokumenteres. Forbedrings- og læringspunkter som avdekkes i evalueringen må følges opp og konkretiseres i en oppfølgingsplan. Virksomhetene skal utarbeide en ledelsesforankret oppfølgingsplan. Som minimum skal den inneholde:

- Læringspunkter
- Konkret beskrivelse av tiltak
- Tidsramme/frist for gjennomføring av tiltak
- Ansvarlig for hvert enkelt tiltak

Oppfølgingen av en hendelse er ikke å anse som avsluttet før samtlige punkter i oppfølgingsplanen er fulgt opp.

4.5 Annet regelverk knyttet til sikring av liv og helse og materielle verdier i virksomhetene

Virksomhetene i sektoren må etterleve en rekke ulike regelverk som har som hensikt å sikre verdier som liv og helse og materielle verdier. KDs krav til arbeidet med samfunnssikkerhet stiller derfor ikke krav til denne type arbeid spesifikt, men heller til de overordnede grunnelementene i beredskapsarbeidet (ROS-analyser, planverk, øvelser mm.). Det er virksomhetenes eget ansvar å sette seg inn i relevant regelverk som omfatter dem. Dette inkluderer blant annet regelverk knyttet til brannvern (forskrift om brannforebygging), helse-, miljø og sikkerhet (internkontrollforskriften), arbeid med kjemiske og biologiske risikofaktorer og andre arbeidsmiljøforhold (forskrift om utførelse av arbeid), smittevern (smittevernloven), helseberedskap (helseberedskapsloven) og tilpasning til natur- og miljøforhold (plan- og bygningsloven).

Det er virksomhetenes eget ansvar å iverksette konsekvens- og sannsynlighetsreduserende tiltak for hendelser med høy risiko. Dette kan for eksempel være å iverksette nødvendige terrorsikringstiltak[27] eller ulike tilgangsstyringsløsninger.

Veiledningsmateriell for arbeidet med samfunnssikkerhet
Noe veiledningsmateriell er referert til i de foregående kapitlene. Annet er tilgjengelig ved å følge lenker i 7.3. I dette avsnittet trekker vi frem noe veiledningsmateriell av særskilt relevans for sikkerhets- og beredskapsarbeidet, I tillegg omtales materiale fra Beredskapsrådet og sikresiden.no separat i henholdsvis 7.1 og 7.2.

[27] Terrorsikring – en veileder i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015)

Veiledere for beredskap ved barnehager og utdanningsinstitusjoner

- Hvordan håndtere alvorlige hendelser i barnehage og skole er utarbeidet av Udir, DSB, Politidirektoratet (POD) og Helsedirektoratet og gir råd om praktisk beredskapsarbeid. Veilederen inneholder informasjon om ansvar, hvordan lage beredskapsplan samt konkrete strategier og forslag til tiltak.

POD oppfordrer virksomheter som har behov for bistand fra politiet med utarbeidelse av lokale beredskapsplaner eller til forebyggende rådgivning til å ta kontakt med politikontakten i sin geografiske enhet på telefon 02800.

- Veileder om atomhendelser for barnehager og skoler er utarbeidet av Udir, Helsedirektoratet og Direktoratet for strålevern og atomberedskap (DSA) i mars 2025. Barn og unge er særlig sårbare for stråling og radioaktivitet. Det er derfor viktig å sikre dem så god beskyttelse som mulig. Denne veilederen skal bidra til at skoler, barnehager og andre som driver opplæringstilbud for barn og unge er best mulig forberedt på atomhendelser. I forbindelse med arbeidet med veilederen ble det også laget et sett med spørsmål og svar om atomhendelser for barnehager og skoler.

Veiledere for beredskap knyttet til terrortrusselen

- Terrorsikring: Veileder i sikkerhets- og beredskapstiltak mot tilsiktede uønskede handlinger er utarbeidet av PST, POD og NSM. Veilederen gir virksomhetene et hjelpemiddel til å utarbeide tidsbegrensede sikkerhetstiltak for å møte en terrortrussel. Behovet for å iverksette slike tiltak kan oppstå ved endringer i trussel- og risikobildet knyttet til mulige terrorhandlinger. Det er stor variasjon når det gjelder de ulike virksomhetenes sikkerhetsbehov. Noen er mer utsatte enn andre avhengig av virksomhetens formål, driftsform og lokalisering. Derfor vil også anbefalte sikkerhetstiltak variere.
- Råd mot terrorhandlinger er også utgitt av PST, POD og NSM. Her gis råd om hva en kan gjøre for å beskytte seg mot terror og andre alvorlige hendelser som kan true liv og helse. Rådene er rettet mot grupper som kan være utsatt for terror og andre alvorlige hendelser, og som ikke nødvendigvis har kunnskap om sikkerhets- og beredskapsarbeid. Dette kan for eksempel være tros- og livssynssamfunn og minoritetsmiljøer, men også andre samlingssteder kan være utsatt.

Veiledning i forebygging av radikalisering og ekstremisme

- Regjeringen har utarbeidet en nasjonal veileder for forebygging av radikalisering og voldelig ekstremisme og en handlingsplan mot radikalisering og voldelig ekstremisme. Målet er å fange opp personer i risikosonen så tidlig som mulig og møte dem med tiltak som virker. Flere sektorer bidrar i oppfølgingen av tiltakene. KD har et særlig ansvar for forebyggende mot gruppebaserte fordommer, fremmedfrykt, rasisme, antisemittisme, hatefulle ytringer, ekstremisme og udemokratiske holdninger. Dette gjøres blant annet gjennom å bygge demokratisk kompetanse, med inkludering og deltakelse, kritisk tenkning og mangfoldskompetanse. I Meld. St. 13 (2024–2025) Forebygging av ekstremisme. Trygghet, tillit, samarbeid og demokratisk motstandskraft fra mars 2025 lanserer regjeringen en rekke tiltak. Et av

tiltakene er et nytt nasjonalt senter for innsats mot radikalisering og voldelig ekstremisme. Sentrale oppgaver for senteret vil være veiledning og støtte til kommuner og førstelinjetjenester, pårørende, nærstående og andre aktører. Senteret skal formidle kompetanse og kunnskap om fenomener, utviklingstrekk og forebyggende arbeid til nasjonale, regionale og lokale aktører. Når senteret er på plass vil det kunne være et relevant tilbud for aktører i kunnskapssektoren.

5 Krav og forventninger til virksomhetenes arbeid med nasjonal sikkerhet

Kunnskapssektoren forvalter og skaper verdier som er strategisk viktige for Norge. Disse verdiene kan også være utsatt for interesse og påvirkning som kan være i strid med nasjonal sikkerhet. Et mer krevende trusselbilde gjør at virksomheter i sektoren må vurdere sin rolle i et nasjonalt sikkerhetsperspektiv.

Samtidig er åpenhet og internasjonalt samarbeid innen høyere utdanning og forskning helt sentralt for å videreutvikle Norge som kunnskapsnasjon. Dette kan være en krevende balanse i praksis, og det er flere hensyn å ta. En forutsetning for å lykkes på dette området er systematisk og risikobasert arbeid med forebyggende sikkerhet. Verdier med betydning for nasjonal sikkerhet må identifiseres, og det må gjennomføres forholdsmessige sikringstiltak, slik at virksomhetene og sektoren jobber under og samarbeider innenfor et akseptabelt risikonivå.

I arbeidet med nasjonal sikkerhet er det flere departementer som har kryssende ansvarsområder, og arbeidet berører i stor grad etterlevelse av regelverk som eies av andre departementer enn KD. Regelverkene som gjør seg gjeldende for kunnskapssektoren er særlig lov om nasjonal sikkerhet (sikkerhetsloven), lov om kontroll med eksport av strategiske varer, tjenester og teknologi mv. (eksportkontrolloven), og lov om gjennomføring av internasjonale sanksjoner (sanksjonsloven), samt tilhørende forskrifter. Dette er regelverk som treffer virksomhetene i ulik grad. Virksomhetene er selv ansvarlige for å sette seg inn i de ulike regelverkene og hvordan disse treffer dem.

Under følger en oversikt over kravene som kommer frem i dette kapittelet til virksomheter som er underlagt sikkerhetsloven.

Tema	Alle virksomheter i sektoren som er underlagt sikkerhetsloven skal:
Styringssystem for sikkerhet	• Etablere og vedlikeholde et styringssystem for sikkerhet som sørger for at virksomheten oppfyller kravene gitt i eller med hjemmel i loven • Samordne styringssystemet med ledelsessystem for informasjonssikkerhet og med virksomhetsstyringen for øvrig. • Dokumentere styringssystemet skriftlig og revidere ved behov.
Sikkerhetsklarerte og autoriserte	• Føre oversikt over virksomhetens ansatte som er sikkerhetsklarert og/eller autorisert iht. sikkerhetsloven. Oversikten skal til enhver tid være oppdatert.
Skjermingsverdige verdier	• Vurdere, kartlegge og holde oversikt over virksomhetens skjermingsverdige verdier (definert som skjermingsverdig informasjon, informasjonssystemer, infrastruktur eller objekter).[28]
Sikkerhetsgradert informasjon	• Kunne motta og håndtere sikkerhetsgradert informasjon til minimum BEGRENSET.

[28] Virksomhetssikkerhetsforskriften § 2.

5.1 Lov om nasjonal sikkerhet (sikkerhetsloven)

Sikkerhetsloven skal bidra til å trygge *nasjonale sikkerhetsinteresser* og forebygge, avdekke og motvirke sikkerhetstruende virksomhet. Loven skal også bidra til at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.[29]

Sikkerhetsloven gjelder for statlige, fylkeskommunale og kommunale organer. Alle KDs underliggende virksomheter er derfor direkte underlagt sikkerhetsloven. Loven gjelder også for leverandører av varer og tjenester i forbindelse med sikkerhetsgraderte anskaffelser. Ved behov fatter KD vedtak om at loven helt eller delvis skal gjelde for øvrige virksomheter innenfor departementets ansvarsområde, jf. § 1-3.

5.2 Styringssystem for sikkerhet

Alle virksomheter som omfattes av sikkerhetsloven skal ha et dokumentert styringssystem for sikkerhet.[30] Kravet gjelder uavhengig av om virksomheten har skjermingsverdige verdier. Styringssystemet skal omfatte alle aktiviteter med betydning for forebyggende sikkerhetsarbeid. Herunder aktiviteter dedikert for sikkerhet og aktiviteter som kan ha betydning for sikkerhet. Styringssystemet bør dekke:

- Risikostyring
- Sikkerhetsledelse
- Sikkerhetsorganisering
- Sikkerhetstiltak og -prosedyrer
- Forholdet til andre virksomheter
- Sikkerhetsoppfølging
- Sikkerhetsdokumentasjon

Styringssystemet skal sørge for at virksomheten oppfyller kravene gitt i eller med hjemmel i loven. Utformingen må tilpasses verdiene som skal beskyttes og dimensjoneres med hensyn til risiko for sikkerhetstruende virksomhet. Hva som kreves for å oppnå dette vil variere fra en virksomhet til en annen, og det kan være store forskjeller mellom hva som kreves av de ulike virksomhetene i KDs sektor.

Styringssystemet skal være samordnet med ledelsessystem for informasjonssikkerhet og virksomhetsstyringen for øvrig. Det innebærer at arbeidet med informasjonssikkerhet skal sees i sammenheng med øvrig arbeid med sikkerhet og beredskap, og at det helhetlige sikkerhetsarbeidet skal være innarbeidet i virksomhetsstyringen på en hensiktsmessig måte.

Styringssystemet skal gjennomgås årlig, og revideres ved behov. NSM har utarbeidet en veileder i sikkerhetsstyring som kan benyttes. Digitaliseringsdirektoratets veileder for helhetlig styring og kontroll av informasjonssikkerhet kan benyttes i arbeidet med å utforme et helhetlig styringssystem for sikkerhet.

[29] Sikkerhetsloven § 1-1.

[30] Virksomhetssikkerhetsforskriften § 3.

5.3 Sikkerhetsklarering og autorisasjon

Virksomheter underlagt sikkerhetsloven må kunne motta og behandle sikkerhetsgradert informasjon. Loven stiller krav til hvordan slik informasjon skal håndteres. Herunder må virksomheten ha ansatte som er sikkerhetsklarert og/eller autorisert for aktuelt nivå.

Personer som skal ha tilgang til sikkerhetsgradert informasjon, må autoriseres. Personer som skal autoriseres for tilgang til informasjon gradert KONFIDENSIELT eller høyere, må ha gyldig sikkerhetsklarering.[31]

Den enkelte virksomhet har ansvaret for at ansatte har tilstrekkelig sikkerhetsklarering og autorisasjon. Følgende rutiner gjelder for sikkerhetsklarering og autorisasjon av ansatte i virksomheter underlagt KD:

- Sikkerhetsklarering gjennomføres av Sivil klareringsmyndighet (SKM). Ved behov for sikkerhetsklarering oversendes søknad med begrunnelse og ferdig utfylt personopplysningsblankett til KD. Departementet er anmodende myndighet og fremmer søknaden for SKM etter vurdering.
- Autorisasjon gjennomføres i den enkelte virksomhet. Foruten de krav og vilkår som følger av sikkerhetsloven med forskrifter stiller KD krav til at to vilkår må være innfridd før KDs underliggende virksomheter kan gjennomføre autorisasjon av egne medarbeidere: (1) Virksomheten har et dokumentert styringssystem for sikkerhet, og (2) virksomhetens autorisasjonsansvarlig er autorisert av KD. Virksomhetens leder er autorisasjonsansvarlig.[32] Ved behov kan autorisasjonsansvaret delegeres internt i virksomheten.

Mer informasjon om sikkerhetsklarering og autorisasjon finnes på nsm.no.

5.4 Grunnleggende nasjonale funksjoner

Grunnleggende nasjonale funksjoner (GNF) er tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.

KD skal identifisere og holde oversikt over GNF innenfor departementets ansvarsområde. *Kunnskapsdepartementets virksomhet, handlingsfrihet og beslutningsdyktighet* er utpekt som en GNF. I tillegg er det utpekt en GNF innenfor *forskning og utvikling*. Sistnevnte er under arbeid.

[31] Sikkerhetsloven § 8-1.

[32] Sikkerhetsloven § 8-9.

5.5 Skjermingsverdige verdier

Virksomhetssikkerhetsforskriften definerer skjermingsverdige verdier som: skjermingsverdig informasjon, skjermingsverdige informasjonssystemer, skjermingsverdig infrastruktur og skjermingsverdige objekter[33].

KD skal innenfor sitt ansvarsområde utpeke, klassifisere og holde oversikt over skjermingsverdige objekter og infrastruktur. Objekter og infrastruktur er skjermingsverdige dersom det enten kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse, eller kan skade nasjonale sikkerhetsinteresser på annen måte[34].

Identifisering av skjermingsverdige objekter eller infrastruktur kan skje på to måter:

(1) Virksomheten identifiserer et objekt eller en infrastruktur virksomheten mener kan være skjermingsverdig og melder dette til KD.

(2) KD identifiserer et objekt eller en infrastruktur som departementet mener kan være skjermingsverdig og tar kontakt med den relevante virksomheten.

Ved behov vil KD gi virksomheten i oppdrag å skadevurdere verdien. Dersom verdien utpekes som skjermingsverdig, stiller sikkerhetsloven krav om etablering av et forsvarlig sikkerhetsnivå. Det innebærer at det skal være samsvar mellom risiko og tiltak.

5.6 Sikkerhetstruende investeringer og oppkjøp

Utenlandske investeringer i, og oppkjøp av, norske virksomheter kan benyttes for å få innsikt i sensitiv informasjon og tilgang til teknologi og ressurser av strategisk betydning.

For de av KDs underliggende virksomheter som omfattes av sikkerhetsloven, kan utfordringer knyttet til sikkerhetstruende investeringer og oppkjøp håndteres gjennom bestemmelsene om eierskapskontroll i sikkerhetsloven kapittel 10.

Sikkerhetsloven § 2-5 kan benyttes overfor alle virksomheter, også de som ikke er underlagt sikkerhetsloven. Bestemmelsene her kan også anvendes ved aktiviteter som ennå ikke er satt ut i livet, men som har potensial til å innebære en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet.

Varslings- og meldeplikt
Virksomheter som er underlagt sikkerhetsloven har varslings- og meldeplikt til overordnet myndighet etter følgende bestemmelser:

- Sikkerhetsloven § 4-5: Varslingsplikt om sikkerhetstruende hendelser.
- Sikkerhetsloven § 9-4: Varslingsplikt om anskaffelser til skjermingsverdig informasjonssystem, objekt eller infrastruktur.
- Sikkerhetsloven § 10-1: Meldeplikt om erverv av virksomhet.

[33] Virksomhetssikkerhetsforskriften § 2.

[34] Sikkerhetsloven § 7-1 første ledd.

For å vurdere om det foreligger en mulig sikkerhetstruende aktivitet, kan følgende spørsmål være til hjelp:

- Er investoren kontrollert av en annen stats myndigheter?
- Har investoren tilknytning til en stat som er omtalt i E-tjenestens trusselvurdering, PSTs trusselvurdering og/eller NSMs risikovurderinger?
- Gjelder saken sensitiv teknologi eller informasjon?
- Har saken konsekvenser for kritisk infrastruktur, i tilfeller hvor virksomheten ikke er underlagt sikkerhetsloven?
- Vil saken kunne få konsekvenser for sikkerheten i kritiske forsyningskjeder?
- Ligger virksomheten på, eller råder den over, strategisk eiendom (eiendom som ligger i nærheten av, eller kan utgjøre en sikkerhetsrisiko for, et skjermingsverdig objekt eller militært område eller tilsvarende) eller ligger nær slik eiendom?
- Er det andre forhold i saken som kan karakteriseres som av betydning for nasjonale sikkerhetsinteresser?

Kontaktpunkter
Nasjonal sikkerhetsmyndighet (NSM) er utpekt som nasjonalt kontaktpunkt for meldinger om utenlandske oppkjøp og investeringer som kan ha konsekvenser for nasjonale sikkerhetsinteresser.

- Varsling om sikkerhetstruende hendelser, jf. § 4-5, skal normalt gå direkte, og uten unødig opphold, fra virksomheten til NSM. Henvendelser kan sendes til: postmottak@nsm.no
- Varsler og meldinger etter de øvrige bestemmelsene, § 9-4 og § 10-1, skal sendes til KD: postmottak@kd.dep.no
- Andre typer henvendelser, varsler eller behov for bistand til å vurdere sakens betydning kan sendes til postmottak@kd.dep.no

For mer informasjon om sikkerhetstruende investeringer og oppkjøp, se NSMs veileder i bruk av sikkerhetsloven for å motvirke sikkerhetstruende investeringer og oppkjøp.

5.7 Forskningssikkerhet og internasjonalt akademisk samarbeid

En åpen og internasjonalt orientert kunnskapssektor er og blir avgjørende for å nå langsiktige kunnskapspolitiske mål, inkludert for å ivareta langsiktige nasjonale kunnskaps- og kompetansebehov, videreutvikle Norge som en konkurransedyktig kunnskapsnasjon og bidra til å finne løsninger på globale utfordringer. Konferanser, forskningsopphold, mobilitet og tilsvarende er kjerneaktiviteter for sektoren. Samtidig skaper og forvalter norske universiteter, høgskoler og forskningsinstitutter kunnskap innenfor sensitive fagområder som er attraktive også utenfor våre grenser, inkludert for stater Norge ikke har sikkerhetspolitisk samarbeid med. De siste årenes trusselvurderinger omtaler norske forskningsinstitusjoner og kunnskaps-

sektoren som mål for fremmede staters etterretningsvirksomhet. Dette foregår ikke bare gjennom avanserte nettverksoperasjoner, men også ved utplassering av studenter på høyere grads nivå, etablering av relasjoner i akademiske arenaer som for eksempel konferanser, invitasjoner til besøk og forskningsopphold, og gjennom andre tilsynelatende transparente og regulerte prosesser. Underliggende virksomheter må derfor være aktsomme og oppmerksomme, for å forebygge at denne typen forsøk på informasjonsinnhenting fører til at verdier som burde beskyttes, havner i feil hender.

I stortingsmeldingen om forskningssystemet Meld. St. 14 (2024–2025) Sikker kunnskap i en usikker verden fra mars 2025 lanseres begrepet *forskningssikkerhet*, som bygger på EUs research security-begrep. EUs definisjon av forskningssikkerhet legger vekt på identifiseringen og håndteringen av risiko knyttet til 1) uønsket kunnskapsoverføring, 2) uønsket påvirkning og innblanding samt 3) brudd på forskningsetikk og faglig integritet gjennom bruk av kunnskap og teknologi til å underminere sentrale samfunnsverdier. EUs arbeid med forskningssikkerhet tar utgangspunkt i etablerte prinsipper for ansvarlig internasjonalisering. Det innebærer blant annet å fremme og forsvare akademisk frihet og institusjonell autonomi, tilrettelegge for fortsatt åpen forskning i tråd med prinsippet «så åpen som mulig, så lukket som nødvendig» og fremme bruk av mest mulig målrettede og proporsjonale tiltak som legger til rette for at risiko skal håndteres, ikke unngås. EUs tilnærming til disse spørsmålene ligger dermed nært opp til den linjen regjeringen har fulgt på dette området i de senere år.

Ansvarlig internasjonalt kunnskapssamarbeid

Internasjonalt samarbeid innen høyere utdanning og forskning er avgjørende for å videreutvikle Norge som kunnskapsnasjon. I tråd med etablerte prinsipper om akademisk frihet og institusjonell selvstendighet er det opp til høyere utdannings- og forskningsinstitusjonene selv å velge hvem de ønsker å inngå samarbeid med. Det er avgjørende at institusjonene har et bevisst forhold til de verdiene de forvalter, og legger til rette for en god balanse mellom åpenhet og aktsomhet når de samhandler med andre land. I dette ligger også et ansvar for å sette seg inn i relevant lovgivning, gjøre egne risiko- og sårbarhetsvurderinger og søke råd hos relevante myndigheter ved behov.

For å tilrettelegge for økt kunnskap og bevissthet om både muligheter, utfordringer og dilemmaer knyttet til internasjonalt samarbeid, har KD tatt initiativ til å utvikle Retningslinjer og verktøy for ansvarlig internasjonalt kunnskapssamarbeid.[35] Retningslinjene er utviklet av HK-dir og Norges forskningsråd som en nettbasert ressurs som oppdateres løpende. Retningslinjene skal bygge opp under institusjonenes eget sikkerhets- og beredskapsarbeid, og være et praktisk verktøy for institusjoner, enkeltforskere og studenter. HK-dir gjennomfører også egne webinarer om ulike temaer og problemstillinger. Målet er at flest mulig blir i stand til å foreta gode kunnskapsbaserte vurderinger av ulike sikkerhetshetsutfordringer man må være forberedt på å møte i sitt internasjonale virke.

[35] Retningslinjer for ansvarlig internasjonalt samarbeid | HK-dir

Retningslinjene skal tilrettelegge for en god balansegang mellom en fortsatt åpen høyere utdannings- og forskningssektor og hensynet til nasjonale interesser i bred forstand. Dette er et sentralt tema i den reviderte Panorama-strategien for samarbeid innen høyere utdanning, forskning og innovasjon med prioriterte land utenfor EU/EØS (2021–2027). Her introduseres ansvarlighet som et grunnleggende prinsipp for internasjonalt akademisk samarbeid, på linje med etablerte prinsipper som kvalitet, relevans, gjensidighet og langsiktighet.

Ulovlig teknologioverføring – eksportkontroll

Norske universiteter og høgskoler skaper og deler kunnskap innenfor fagområder som kan ha både sivil og militær relevans og nytteverdi. Dette omtales som flerbruksteknologi, og er beskyttet av eksportkontrollregelverket. Eksportkontroll i kunnskapssektoren handler i hovedsak om kontroll av teknologioverføring. Begrepet teknologioverføring, fra det engelske begrepet intangible technology transfer, defineres som spesifikk informasjon nødvendig for utvikling, produksjon eller bruk av varer slik disse begrepene er definert i forskriftens vedlegg. Denne informasjonen tar form som tekniske data eller teknisk assistanse. For mer informasjon om hva teknologioverføring innebærer, se Utenriksdepartementets (UD) retningslinjer.

UD er ansvarlig myndighet for gjennomføring av eksportkontrollen i Norge. UD har utarbeidet egne retningslinjer for kunnskapssektoren (2020).[36] Råd for samfunnssikkerhet og beredskap har i tillegg skrevet en kort introduksjon på sine nettsider til eksportkontroll og hvilken betydning det har for kunnskapssektoren.[37] Eksportkontroll omtales videre også i HK-dirs retningslinjer for ansvarlig internasjonalt kunnskapssamarbeid.[38]

I Meld. St. 25 (2023–2024) Eksport av forsvarsmateriell fra Norge i 2023, eksportkontroll og internasjonalt ikke-spredningssamarbeid pekes det på at det er et utviklingstrekk at flere land vi ikke har sikkerhetssamarbeid med forsøker å få tak i kunnskap som er relevant for deres egne militære systemer og kapasiteter fra norske teknologimiljøer. Både PST og Etterretningstjenesten har i sine årlige vurderinger i de senere år vist til at utenlandske aktører målrettet forsøker å anskaffe sensitiv kunnskap fra norske kunnskaps- og teknologimiljøer til militær bruk gjennom fordekte anskaffelser. Dette gjøres blant annet ved å plassere og rekruttere egne borgere i avanserte utdannings- og forskningsmiljøer. Kampen om tilgang til kunnskap og forskning står i sentrum av den geopolitiske rivaliseringen og kappløpet om å omsette ny teknologi til militære kapasiteter. Den teknologiske utviklingen gir oss som nasjon mange muligheter, men også utfordringer. I Norge er høyere utdanning gratis, forskerstillinger er godt lønnet og norske utdannings- og forskningsinstitutter holder et høyt internasjonalt nivå innen kunnskapsområder som har militær bruk eller som kan benyttes i utviklingen av masseødeleggelsesvåpen (MØV). Undervannsteknologi og materialteknologi er eksempler på kunnskap

[36] UD (2020): Retningslinjer for kontroll med kunnskapsoverføring, tilgjengelig på: https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/om-eksportkontroll/kunnskap/id2500543/

[37] Beredskapsrådet (2021): Eksportkontroll i kunnskapssektoren, tilgjengelig på: https://www.uis.no/nb/samarbeid/eksportkontroll-i-kunnskapssektoren

[38] HK-dir (2024): Eksportkontroll, lisens og oppholdstillatelse, tilgjengelig på: Eksportkontroll, lisens og oppholdstillatelse | HK-dir (hkdir.no)

som vi vet utenlandske aktører forsøker å anskaffe fra Norge til militær bruk i hjemlandet. De siste årene er flere forsøk på ulovlig teknologioverføring fra Norge avdekket og hindret.

Regjeringen har sett behov for å styrke eksportkontrollregimet for å svare på de nye utfordringene, og har både satt i gang et arbeid med å tydeliggjøre eksportkontrollforskriften, og har etablert et nytt direktorat under UD, Direktorat for eksportkontroll og sanksjoner (DEKSA). DEKSA skal rustes for å møte saksbehandlings- og veiledningsbehovet for blant annet kunnskapssektoren i forbindelse med teknologioverføring.

UD har sett behov for å tydeliggjøre hvordan eksportkontrollregelverket treffer kunnskapssektoren, og jobber med endringer i eksportkontrollforskriften. UD jobber blant annet med en definisjon av begrepet «teknologi», bestemmelser om lisensplikt for teknologi, og andre type avklaringer spesifikke for kunnskapssektoren. UD skal etter planen ikraftsette endringene i forskriften første halvår 2025, og vil samtidig med dette publisere en veileder for teknologioverføring rettet mot kunnskapssektoren.

Det er ulike måter å jobbe med etterlevelse av eksportkontrollregelverket. Noen kan se fordeler med å integrere arbeidet som en del av virksomhetens systematiske arbeid med sikkerhet, og andre kan anse det som formålstjenlig å inkorporere det i virksomhetens ledelsessystem for informasjonssikkerhet. Vi anbefaler å gjennomgå relevante veiledere nevnt over for dette arbeidet tilpasset kunnskapssektoren. På generelt grunnlag kan KD anbefale at virksomhetene utarbeider gode oversikter over sensitive fagområder og lisenspliktig utstyr i egen organisasjon, for å være forberedt på når det må søkes om lisenser. Virksomhetene bør også innarbeide interne rutiner som ivaretar tilstrekkelig beskyttelse mot ulovlig teknologioverføring, samt sørge for ledelsesforankring av dette arbeidet. Det kan være hensiktsmessig å utnevne roller med særskilt ansvar for å søke om eksportlisenser.

6 Krav og forventninger til sektorens arbeid med informasjonssikkerhet

For å øke virksomheters digitale egenberedskap og gjennom dette Norges samlede digitale motstandskraft, er det viktig at virksomheter følger råd og anbefalinger fra myndighetene.[39] Det er ledelsen ved den enkelte virksomhet som har ansvaret for å etablere og opprettholde tilfredsstillende informasjonssikkerhet. Informasjonssikkerhet skal være en integrert del av det øvrige sikkerhetsarbeidet i virksomheten og skal inngå i den helhetlige virksomhetsstyringen.[40] I kapittel 5 om nasjonal sikkerhet beskrives hvordan arbeidet med informasjonssikkerhet, forebyggende sikkerhetsarbeid og virksomhetsstyring kan samordnes. Det er ledelsen ved den enkelte virksomhet som har ansvar for å sørge for at virksomheten jobber helhetlig med de tre sikkerhetsdomenene og ser dem i sammenheng med hverandre.

Som i kapittel 4 og 5, stilles det flere krav i dette kapittelet. Der det står «skal» må dette leses som «bør» for de virksomhetene som ikke er direkte underlagt departementet. Å kunne dokumentere etterlevelse av krav er en viktig del av internkontrollarbeidet innenfor informasjonssikkerhet.

KDs underliggende virksomheter skal:

Følge gjeldende regelverk som omfatter informasjonssikkerhet (herunder personopplysningssikkerhet), inkludert:

- forvaltningsloven med e-forvaltningsforskriften
- offentlighetsloven med forskrifter
- sikkerhetsloven med forskrifter
- personopplysningsloven med forskrifter
- helseregisterloven med forskrifter
- ekomloven med forskrifter
- e-signaturloven med forskrifter
- reglement for økonomistyring i staten

[39] Fremtidens digitale Norge. Nasjonal digitaliseringsstrategi 2024–2030

[40] Digdir: Helhetlig styring og kontroll av informasjonssikkerhet, tilgjengelig på: https://www.digdir.no/informasjonssikkerhet/helhetlig-styring-og-kontroll-av-informasjonssikkerhet/2284

KDs underliggende virksomheter som er omfattet av KDs styrings-modell for informa-sjonssikkerhet og personvern i høyere utdanning og forskning skal / andre virsomheter i sektoren bør:

Følge kravene i rundskriv F-04-20 Policy for informasjonssikkerhet og person-vern i høyere

- utdanning og forskning. I henhold til policyen skal virksomhetene:
- ha et ledelsessystem for informasjonssikkerhet
- ha oversikt over informasjon og personopplysninger
- gjennomføre risikovurderinger og etablerer sikringstiltak
- etablere løsninger for hendelseshåndtering, lukking av avvik og kontinuitet
- sørge for kontroll med tjenesteleverandører
- ha internkontroll for behandling av personopplysninger
- ivareta de registrertes rettigheter
- utnevne personvernombud
- gjennomføre vurderinger av personvernkonsekvenser (DPIA[41])
- sørge for innebygd personvern og informasjonssikkerhet
- sørge for opplæring og kompetanseheving
- dokumentere arbeidet med informasjonssikkerhet og personvern

Et viktig grunnlag for arbeidet med informasjonssikkerhet, både i KD og i virksom-hetene i sektoren, er: Nasjonal strategi for digital sikkerhet, Nasjonal strategi for digital sikkerhetskompetanse, Strategi for digital kompetanse og infrastruktur i bar-nehage og skole og Strategi for digital omstilling i universitets- og høyskolesektoren, med handlingsplan.

[41] Data Protection Impact Assessment

6.1 Om Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning

Virksomheter som er omfattet av Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern i høyere utdanning og forskning, skal følge kravene i rundskriv F-04-20 Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning.[42] Formålet med policyen er å beskrive hvilke overordnede krav som stilles til arbeidet med informasjonssikkerhet og personvern i virksomhetene. Kravene i policyen følger av lovpålagte krav til arbeidet med informasjonssikkerhet og personvern, og øvrige nasjonale føringer for disse områdene. Policyen går ikke detaljert inn på hvilke regler som gjelder, men oppsummerer de overordnede kravene. Departementet forutsetter at virksomhetene er kjent med gjeldende lovgivning og retningslinjer på området og etterlever disse.[43] Siste versjon av policyen er til enhver tid tilgjengelig på regjeringens nettsider under Kunnskapsdepartementets rundskriv. HK-dir er fagdirektorat for informasjonssikkerhet og personvern i høyere utdanning og forskning og skal følge opp at kravene i policyen etterleves. Sikt er faglig rådgiver for KD og HK-dir innen informasjonssikkerhet og personvern og leverer viktige tjenester som skal styrke sikkerheten i sektoren, i tråd med kravene i policyen.

Virksomhetene som *ikke* er omfattet av styringsmodellen for informasjonssikkerhet og personvern i høyere utdanning og forskning, oppfordres til å se hen til de overordnede kravene beskrevet i policyen.

6.2 Risikostyring og ledelse av informasjonssikkerhet

Gjennom sin kjernevirksomhet skaper, forvalter og deler KDs sektor informasjonsverdier av stor betydning for samfunnet. Eksempler på dette er store mengder personopplysninger og helsedata, og nye banebrytende teknologier og sensitive forskningsområder. Sektoren har verdifulle IKT-infrastrukturer, og svært avanserte informasjonsbærende laboratoriefasiliteter. Med sitt brede samfunnsoppdrag representerer også sektoren tjenester og aktiviteter som er viktige for landets daglige funksjon.

[42] De aktuelle virksomhetene er: alle statlige universiteter og høyskoler, HK-dir, NOKUT, Sikt, Norges forskningsråd, UNIS, Simula, De nasjonale forskningsetiske komiteene og NUPI. Styringsmodellen er tilgjengelig på HK-dir sine nettsider: Styring av informasjonssikkerhet og personvern | HK-dir.

[43] Se oversikter over regelverk i vedlegg til NOU 2018: 14 – IKT-sikkerhet i alle ledd — Organisering og regulering av nasjonal IKT-sikkerhet og i vedlegg til F-04-20 Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning.

Det overordnede målet for informasjonssikkerhet er å beskytte disse informasjonsverdiene gjennom ivaretakelse av informasjonens konfidensialitet, integritet og tilgjengelighet:

- *Konfidensialitet* innebærer at informasjonen ikke blir kjent for uvedkommende
- *Integritet* innebærer at informasjonen ikke blir endret utilsiktet eller av uvedkommende
- *Tilgjengelighet* innebærer at informasjonen er tilgjengelig ved behov

Ulike regelverk krever at konfidensialiteten, integriteten og tilgjengeligheten til informasjon og informasjonssystemer er forsvarlig sikret. I de tilfellene der informasjonssikkerheten kan ha konsekvenser for liv og helse er også fysisk sikkerhet et helt sentralt sikkerhetsmål. Lovverket stiller krav til forsvarlig informasjonsbehandling og riktig beskyttelsesnivå, noe som blir særlig gjeldende i møte med økt digitalisering.

Digitalisering og teknologiutvikling medfører økt effektivisering og fornyelse, men introduserer samtidig nye sårbarheter, avhengigheter og konsentrasjonsrisiko. Sentrale tjenester og funksjoner i samfunnet er i stor grad avhengige av lange og til dels uoversiktlige verdikjeder.[44] Manglende totaloversikt over informasjon, systemer, behandlingsprosesser og mulige sikkerhetshull krever etablering av fungerende helhetlig risikostyring.

Risikostyring av informasjonssikkerhet forutsetter nødvendig oversikt over egne informasjonsverdier, hvilke lovkrav som er knyttet til dem, og hvilke uønskede hendelser og trusler det er som må forhindres. Det innebærer å ha oversikt over egne sårbarheter, og å ha nok kunnskap om truslene som kan utnytte disse sårbarhetene for å ramme informasjonsverdiene. Tekniske sikkerhetstiltak alene vil ikke stoppe trusselaktørene, det er også nødvendig med helhetlig sikkerhetsstyring i virksomheten og god sikkerhetskultur blant brukere av systemer og virksomhetens ansatte. NSM påpeker at ettersom den tekniske sikkerheten blir bedre, kan det gjøre andre metoder for tilgang til informasjon mer attraktive for trusselaktører. Det er derfor viktig å tenke sikkerhet i alle domener, ikke bare det digitale.[45]

Tiltaksområdene omfatter både menneskelige, tekniske og organisatoriske aktiviteter og investeringer, innenfor både IKT-infrastruktur, forsvarlig informasjonsbehandling og arbeidsprosesser, og robuste responsmiljø. Det er nødvendig å bygge en sikkerhetskultur hvor oppmerksomhet og kunnskap om informasjonssikkerhet er en del av den strategiske organisasjonsutviklingen. Informasjonssikkerhet favner dermed bredt, og må sees på som et viktig internkontrollområde og et ledelsesansvar.

Informasjonssikkerhet er et kontinuerlig arbeid, og må gis løpende oppmerksomhet. Alle KDs underliggende virksomheter skal ha et helhetlig ledelsessystem for informasjonssikkerhet.[46] Ledelsessystemet skal være en del av virksomhetens

[44] Meld. St. 9 (2022–2023). Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet.

[45] NSM (2023): Nasjonalt digitalt risikobilde 2023.

[46] Begrepene «ledelsessystem», «styringssystem» og «internkontroll» brukes ofte synonymt når det gjelder styring av informasjonssikkerhetsområdet. Se for eksempel Digitaliseringsdirektoratet: Internkontroll/ styringssystem/ ledelsessystem for informasjonssikkerhet (hentet 05.02.2025).

helhetlige styringssystem for sikkerhet. Omfanget av ledelsessystemet bør tilpasses virksomhetens størrelse og organisering, og de informasjonsverdier, aktiviteter og den egenart som virksomheten besitter. Ledelsessystemet skal beskrive virksomhetens mål og strategier for informasjonssikkerheten, og tydeliggjøre de roller og ansvarsområder som sikkerhetsarbeidet fordeles på. Ledelsessystemet skal beskrive alle de prosesser og aktiviteter en virksomhet samlet skal gjøre av planlagte og systematiske tiltak for risikostyring av informasjonssikkerhet, og være basert på anerkjente standarder som ISO/IEC 27001. Det er toppledelsens ansvar å sørge for at det er nok ressurser til å støtte et tilfredsstillende arbeid med informasjonssikkerhet i virksomheten.

6.3 Håndtering av hendelser

Håndtering av alvorlige informasjonssikkerhetsbrudd og brudd på personopplysningssikkerheten inngår i ledelsessystemet for informasjonssikkerhet. Alle virksomheter må ha en beredskapsplan for å kunne håndtere de hendelsene som kan inntreffe (se også kap. 4.2). Formålet med beredskap er å styrke virksomhetenes motstandsdyktighet når de utsettes for store, negative påkjenninger til tross for forebyggende sikkerhetsarbeid. Beredskap oppnås ved at virksomhetene har planlagt og øvd på hvordan ekstraordinære påkjenninger best kan mestres. Planer og øvelser skal sette virksomhetene i stand til raskt å oppdage, kontrollere, begrense skadene av og forebygge informasjonssikkerhetsbrudd og brudd på personopplysningssikkerheten. Det skal også bidra til at virksomhetene kan videreføre kritiske oppgaver samtidig som håndtering av hendelser og gjenoppretting av normal drift pågår.

En IKT-sikkerhetshendelse kan ha følgekonsekvenser langt ut over den virksomheten som er rammet. Flere virksomheter kan også rammes hver for seg av den samme hendelsen f.eks. når det avdekkes sårbarheter i digitale tjenester som utnyttes bredt av trusselaktører. I et samfunn med en rekke digitale avhengigheter og lange, uoversiktlige verdikjeder stiller dette store krav til effektiv håndtering av alvorlige IKT-sikkerhetshendelser på nasjonalt nivå.[47] NSM har utviklet et rammeverk for å sette samfunnet bedre i stand til å håndtere alvorlige IKT-sikkerhetshendelser som rammer på tvers av sektorer. Rammeverk for håndtering av IKT-sikkerhetshendelser skal bidra til mer effektiv håndtering av alvorlige hendelser, fra virksomhetsnivå til politisk nivå, gjennom god utnyttelse av samfunnets samlede ressurser. Det skal videre bidra til å skape god situasjonsoversikt gjennom aggregering og koordinering av informasjon om alle relevante IKT-sikkerhetshendelser.

KD har innført dette rammeverket for virksomhetene som er omfattet av KDs styringsmodell for informasjonssikkerhet og personvern i høyere utdanning og forskning.[48] Cybersikkerhetssenter for forskning og utdanning i Sikt er utpekt som sektorvist responsmiljø for virksomheter underlagt rammeverket. Disse virksomhetene har egne lokale responsteam, og et tett samarbeid med sektorvist

[47] JD (2015): NOU 2015: 13 – *Digital sårbarhet – sikkert samfunn*, tilgjengelig på: https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

[48] HK-dir (2023): Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren.

responsmiljø gjør at disse nå er bedre forberedt til å håndtere fremtidige trusler og hendelser. I 2022 ble også Udir og Statped underlagt rammeverket.

6.4 Forsvarlig behandling av personopplysninger

Alle virksomheter som behandler personopplysninger, skal føre protokoll over de ulike behandlingsaktivitetene de har ansvar for. Denne vil være et viktig grunnlag for arbeidet med informasjonssikkerhet, som i denne sammenheng handler om å sørge for at all behandling av personopplysninger blir ivaretatt på en tilfredsstillende måte. Dette gjøres ved først å identifisere hvilke personopplysninger virksomheten har. Deretter gjennomføres en risikovurdering for å avklare om eksisterende sikkerhetstiltak er tilfredsstillende.[49]

Behandling av personopplysninger forutsetter tilpassede informasjonssikkerhetstiltak. I henhold til personopplysningsforordningen (GDPR) skal sikringstiltakene være tilpasset opplysningenes art, omfang, behandlingsformål og behandlingskontekst. Det skal tas hensyn til både sannsynlighet for og konsekvens av eventuelle brudd på personopplysningssikkerheten når sikringstiltak velges. Virksomhetene skal kunne dokumentere at personopplysninger behandles i tråd med personvernprinsippene, jf. artikkel 5 i personvernforordningen.[50] Dette gjøres ved å etablere og vedlikeholde tiltak for å sikre at personopplysningene behandles i samsvar med regelverket, ved å etablere internkontroll for behandling av personopplysninger. Internkontrollen bør ses i sammenheng med ledelsessystemet for informasjonssikkerhet, og den øvrige virksomhetsstyringen. Virksomhetene har varslingsplikt til Datatilsynet og den registrerte personen ved brudd på personopplysningssikkerheten.

6.5 Særlig om tjenesteutsetting

Det må gjøres særskilte vurderinger når en skal sette ut tjenester til eksterne leverandører, som for eksempel ved bruk av skytjenester.[51] NSM er bekymret for tjenesteutsetting av samfunnskritiske IKT-tjenester uten tilstrekkelige risikovurderinger og sikringstiltak, og at data flyttes til utlandet uten tilstrekkelige sikkerhetsfaglige vurderinger. NSM har utarbeidet temarapporten Sikkerhetsfaglige anbefalinger ved tjenesteutsetting, med anbefalinger til offentlige og private virksomheter som vurderer å tjenesteutsette basisdrift, applikasjonsdrift eller applikasjonsforvaltning til en ekstern tjenesteleverandør.

Tjenesteutsetting som omfatter overføring av personopplysninger ut av EØS, til såkalte tredjeland, krever et særskilt grunnlag for å være lovlig. Virksomheten må ha identifisert om det finnes et overføringsgrunnlag før personopplysningene overføres til et tredjeland eller til en internasjonal organisasjon. Hvis det ikke finnes, er overføringen ulovlig. Det gjelder også hvis overføringsgrunnlaget ikke vil fungere i

[49] Datatilsynet (2018): Informasjonssikkerhet og internkontroll, tilgjengelig på: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/

[50] Datatilsynet: Personvernprinsippene (hentet 05.02.2025).

[51] NOU 2015: 13 – *Digital sårbarhet – sikkert samfunn*.

praksis. Hvis overføringsgrunnlaget ikke sikrer god nok beskyttelse for personopplysningene i seg selv, må man i tillegg iverksette andre tiltak. Formålet er å sikre at personopplysningsvernet blir det samme ved overføring til stater som ikke har det samme beskyttelsesnivået, som innenfor EØS-området.[52]

Overføring av personopplysninger til USA har vært utfordrende etter at den tidligere avtalen som regulerte slike overføringer ble kjent ugyldig i den såkalte Schrems II-dommen 16.7.20. I juli 2023 vedtok EU nye regler som gjør det enklere å overføre personopplysninger til USA gjennom det såkalte «EU-US Data Privacy Framework». Dette gjør det mulig å overføre personopplysninger på samme måte som til europeiske virksomheter til amerikanske virksomheter som står på en liste over godkjente virksomheter. De amerikanske virksomhetene må fortsatt følge de andre reglene i personvernforordningen, som å ha behandlingsgrunnlag eller databehandleravtaler.[53] Virksomheter som ønsker å overføre personopplysninger til amerikanske virksomheter med godkjenning, må fremdeles vurdere om det foreligger tilstrekkelig overføringsgrunnlag.

For veiledning om forpliktelser ved overføring av personopplysninger utenfor EØS, henstiller vi virksomhetene til å rådføre seg med Datatilsynet, og holde seg orientert om veiledningsmaterialet på deres nettsider. Direktoratet for forvaltning og økonomistyring (DFØ) har også utviklet en veiledning om overføring av personopplysninger til USA.

Reglene om overføring av personopplysninger ut av EØS kommer i tillegg til alle de andre forpliktelsene etter forordningen.[54]

6.6 Veiledningsressurser for arbeidet med informasjonssikkerhet

Det er utviklet et fellesprodukt med ti anbefalte tiltak som virksomheter i offentlig og privat sektor bør gjennomføre – se kapittel 3 i tiltaksoversikten til Nasjonal strategi for digital sikkerhet. Tiltakene er hentet frem gjennom et samarbeid bestående av virksomheter fra både offentlig og privat sektor. Tiltakene gir norske virksomheter et godt utgangspunkt for hva de bør tenke på, uavhengig av størrelse, modenhet og kompetanse om informasjonssikkerhet.

NSMs Grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. De er et utvalg av de prinsippene og tiltakene NSM mener er mest relevante for norske virksomheter, men de omfatter ikke alle tenkelige tiltak. Utvelgelsen er gjort i samarbeid med norske offentlige og private virksomheter. Ved å iverksette de anbefalte tiltakene mener NSM at virksomheter vil etablere et godt forsvar mot cybertrusler, men det er ingen garanti for at de ikke blir rammet.

---

52 Datatilsynet (2021): Overføring av personopplysninger ut av EØS, tilgjengelig på: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/

53 Datatilsynet (2023): Nye regler for overføring av personopplysninger til USA | Datatilsynet

54 Datatilsynet: Virksomhetens plikter (hentet 13.02.2025)

Datatilsynet har utarbeidet en rekke veiledere, blant annet om internkontroll og informasjonssikkerhet, som kan være nyttige for virksomhetene i kunnskapssektoren. For veiledning i gjennomføringen av ledelsessystem for informasjonssikkerhet, viser departementet til Digitaliseringsdirektoratets praktisk rettede veiledningsmateriell for internkontroll i praksis – informasjonssikkerhet og veiledningstjenestene til Sikt.

HK-dir gjennomfører årlige kartlegginger av arbeidet med informasjonssikkerhet og personvern hos virksomhetene som er underlagt Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern i høyere utdanning og forskning. På bakgrunn av dette mottar disse virksomhetene anbefalinger fra HK-dir for det videre arbeidet, som det forventes at de følger. HK-dir utgir resultatene fra kartleggingen i en årlig risiko- og tilstandsrapport, som kan benyttes til å vurdere egen etterlevelse av *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning* opp mot tilstanden i sektoren. Virksomhetene oppfordres også til å legge vurderingene av risiko i rapporten til grunn for sin egen risikostyring på informasjonssikkerhets- og personvernområdet. HK-dir utgir også temarapporter om utvalgte tema.[55]

Cybersikkerhetssenteret for forskning og utdanning ble etablert i 2021 og ligger under Sikt. Cybersikkerhetssenteret utvikler sektortilpassede tiltak og tjenester innenfor tre hovedområder: *Analyse, respons* og *rådgiving*. Områdene utfyller hverandre og tilbyr helhetlige og målrettede leveranser til sektoren. Leveransene skal bidra til at virksomhetene kan møte de føringer som er gitt i gjeldende *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning*. Cybersikkerhetssenteret har også rollen som «sektorvist responsmiljø», i henhold til *Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren*. I arbeidet med sikkerhetskultur og opplæring anbefaler KD at universiteter og høyskoler benytter seg av de kurs og opplæringstilbud som Cybersikkerhetssenteret tilbyr.

Nasjonalt cybersikkerhetssenter (NCSC) i NSM er den nasjonale responsfunksjonen for alvorlige digitale angrep. NCSC er knutepunkt for nasjonalt og internasjonalt samarbeid innen deteksjon, håndtering, analyse og rådgivning knyttet til digitale angrep.

NSM tilbyr også konkrete tjenester for å redusere sårbarheten for dataangrep. Blant disse er varslingssystem for digital infrastruktur (VDI), et nasjonalt sensornettverk på internett. I første omgang var sensornettverket rettet mot å avdekke forsøk på datainnbrudd mot kritisk infrastruktur. NSM anbefaler nå at også virksomheter som ikke har kritisk infrastruktur vurderer å skaffe seg en slik sensor. I den sammenheng har KD bedt alle sine underliggende virksomheter om å vurdere egen risiko og sårbarhet, for på denne bakgrunn å avgjøre om den enkelte bør søke om deltakelse i VDI.

KD anbefaler at sektoren benytter de ressurser innenfor informasjonssikkerhet som utvikles og tilgjengeliggjøres gjennom Sikresiden.no. Digitaliseringsdirektoratet har

[55] Se for eksempel HK-dirs temarapport fra 2021om Ledelsens styring og kontroll av arbeidet med informasjonssikkerhet for råd om hvordan ledelsens gjennomgang kan gjennomføres.

også en samling ressurser om informasjonssikkerhet som virksomheter i sektoren kan dra nytte av.

Prosjektet «SkoleSec», hvor kommuner og fylkeskommuner har gått sammen om å styrke arbeidet med personvern og informasjonssikkerhet knyttet til digitalt læringsmiljø i grunnopplæringen, tilbyr veiledere og ressurser for kompetanseutvikling. Her finnes også den nasjonale vurderingen av personvernkonsekvenser (DPIA) for Google Workspace for Education, som er gjennomført av KS i samarbeid med Bergen kommune. Foreningen kommunal informasjonssikkerhet (KiNS) har som formål å bidra til økt informasjonssikkerhet i kommuner og fylkeskommuner, og tilbyr kurs og verktøy til bruk i lokalt arbeid med informasjonssikkerhet.

7 Andre ressurser

7.1 Beredskapsrådet

I 2017 oppnevnte KD Råd for samfunnssikkerhet og beredskap i kunnskapssektoren (Beredskapsrådet), som er et frivillig tiltak for å styrke arbeidet med samfunnssikkerhet og beredskap i et bredt lag av kunnskapssektoren.

Rådet har 14 medlemmer bestående av representanter for statlige og private universiteter og høy-skoler, fagskoler, studentsamskipnader og folkehøgskoler, i tillegg til KDs underliggende direktorater/etater. Leder for rådet velges blant medlemmene for en periode på normalt tre år. Universitetet i Stavanger (UiS) ivaretar sekretariatsfunksjonen for rådet og er kontaktpunkt mot KD.

En prioritert oppgave for rådet er å utvikle og dele kunnskap og beste praksis på områder der det vurderes hensiktsmessig, og bidra til erfaringsdeling og samordning mellom virksomhetene. Rådet synliggjør relevant informasjon og kunnskap via egen nettside, sosiale medier, webinarer og konferanser. Eksempler på tema rådet kan ta opp er risiko- og sikkerhetsstyring, ROS-analyser, beredskapsplanverk og -øvelser, fysisk sikring, informasjonssikkerhet og ansvarlig internasjonalt samarbeid, samt andre temaer med grenseflater mot samfunnssikkerhet og beredskap, som forebygging av radikalisering og voldelig ekstremisme blant studenter.

I forbindelse med sistnevnte tema har Beredskapsrådet utgitt råd og anbefalinger (2023) for hvordan utdanningsinstitusjonene kan forebygge radikalisering og voldelig ekstremisme. Denne erstatter «Tiltakslisten» som ble utarbeidet av Beredskapsrådet i 2019 på oppdrag fra KD. Beredskapsrådet har samarbeidet med sikresiden.no om informasjon om dette temaet. Beredskapsrådet har også publisert en Veileder i risiko- og sårbarhetsanalyser for kunnskapssektoren (2022).

7.2 Sikresiden.no

En forutsetning for forebyggende sikkerhetsarbeid og hensiktsmessig håndtering av kritiske situasjoner, er den enkeltes personlige handlingskompetanse. Både ansatte og studenter må vite hva de selv kan gjøre i ulike situasjoner og hvor de kan få hjelp. Enkel tilgang til relevant informasjon og sikkerhetsopplæring er derfor avgjørende. Det bidrar både til å redusere risiko og til å oppfylle lovkrav.

Sikresiden.no er en webapp som er laget av og for UH-sektoren. Den gir studenter og ansatte en felles inngang til hva de selv kan gjøre forebyggende og når noe skjer. Informasjonen er lett å finne og enkel å bruke i konkrete situasjoner. Ved å velge sitt eget studiested, får man også tilgang til lokal informasjon. Sikresiden.no kan være en sentral ressurs i virksomhetens arbeid med å operasjonalisere styrings- og internkontrollsystemer slik at de virker i hele organisasjonen.

Med sikresiden.no har sikkerhetspersonell i UH-sektoren også fått etablert en infrastruktur for deling og gjenbruk, som er tilrettelagt for samarbeid om felles informasjon og opplæringsressurser som e-læring og kunnskapsspill. Dette legger grunn-

laget for en mer helhetlig sikkerhetskultur i UH-sektoren og sparer den enkelte virksomhet for mye arbeid. Alt innhold utvikles i aktivt samarbeid med fagpersoner fra UH-sektoren, med støtte fra nasjonale fagmyndigheter. Innholdet gjøres tilgjengelig på både norsk, engelsk og samisk. I 2025 har om lag 350 000 studenter og ansatte i mer enn 30 virksomheter i UH-sektoren tilgang til brukervennlig informasjon og opplæring innenfor samfunnssikkerhet gjennom sikresiden.no.

For å utnytte potensialet i opplæringsressursene fra sikresiden.no må de brukes systematisk i virksomhetsprosesser der det hører hjemme. Det anbefales at sikresiden.no innlemmes i virksomhetens informasjons- og opplæringsarbeid, for eksempel i forbindelse med opplæring av nye ansatte, studenter og faddere. Sikresiden.no kan også benyttes i mer målrettet opplæring, for eksempel knyttet til hva man kan gjøre i en truende situasjon, en skoleskytings- eller terrorsituasjon, ved selvmordsfare, forebygging av ekstremisme, i arbeidet med å redusere innsiderisiko, brannforebygging, før utenlandsreiser, i personvern- og informasjonssikkerhetsopplæring, samt brukes i sikkerhetsmåneden og i beredskapsøvelser.

Arbeidet med utvikling, drift og forvaltning av sikresiden.no ledes fra OsloMet, og alle som deltar i sikresiden-samarbeidet spleiser på utgiftene.

7.3 Nyttige lenker

Nedenfor følger en liste over aktuelle offentlige virksomheter med oppgaver eller tilbud innenfor samfunnssikkerhet og beredskap og lenke til de mest aktuelle delene av deres nettsider. Listen er ikke uttømmende.

- Beredskapsrådet: Rådet for samfunnssikkerhet og beredskap i kunnskapssektoren
- Datatilsynet: Personvern
- Digitaliseringsdirektoratet (Digdir): Veiledere om informasjonssikkerhet
- Direktoratet for samfunnssikkerhet og beredskap (DSB): Risiko, sårbarhet og beredskap
- Direktoratet for samfunnssikkerhet og beredskap (DSB): Kurssenteret
- Direktoratet for strålevern og atomberedskap (DSA): Atomberedskap
- Etterretningstjenesten: Trusselvurdering Fokus
- Helsedirektoratet: Forskrift om miljø og helse i barnehagen, skoler og skolefritidsordninger
- Justis- og beredskapsdepartementet: Generelt om samfunnssikkerhet
- Kunnskapsdepartementet: Generelt om samfunnssikkerhet i kunnskapssektoren
- Kunnskapssektorens tjenesteleverandør (Sikt): Direktoratet for IKT og fellestjenester i høyere utdanning og forskning
- Nasjonalt fagskoleråd: Risiko og beredskap i høyere yrkesfaglig utdanning
- Nasjonal sikkerhetsmyndighet (NSM): Regelverk og hjelp, inkludert årlige risikovurderinger
- Norsk brannvernforening: Informasjon, opplæring og rådgivning om brannvern
- Norsk Senter for Informasjonssikring (NorSIS): Veiledere, seminarer/konferanser om internkontroll og informasjonssikkerhet
- Politiet: Politiets trusselvurdering
- Politiets sikkerhetstjeneste (PST): Trusselvurderinger og informasjon
- NSM, Politiet, PST: Råd mot terrorhandlinger
- Sikresiden: Sikresiden.no
- Utdanningsdirektoratet: Sikkerhet og beredskap

Utgitt av: Kunskapsdepartementet

Bestilling av publikasjoner:
Departementenes sikkerhets- og serviceorganisasjon
publikasjoner.dep.no
Telefon: 22 24 00 00
Publikasjoner er også tilgjengelige på:
www.regjeringen.no

Design: Departementenes sikkerhets- og serviceorganisasjon