Kunnskapsdepartementet

Desember 2021

Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor

Innhold

Forord

Det norske samfunnet oppleves som trygt for de fleste av oss. Likevel inntreffer det fra tid til annen hendelser som rokker ved denne tryggheten. Det kan være store ulykker, pandemier, klimaproblemer, eller tilsiktede handlinger fra mennesker. De store teknologiske endringene gir oss også en del utfordringer. Denne virkeligheten krever at aktører på ulike nivåer arbeider systematisk med samfunnssikkerhet og beredskap.

Sikkerhet og beredskap berører oss alle, noe som ikke minst har blitt belyst gjennom pandemien som vi i skrivende stund fortsatt står i . Å ivareta sikkerhet og beredskap er et lederansvar. Kunnskapsdepartementet har det overordnede ansvaret for sikkerhet og beredskap innenfor hele departementets politikkområde. For at vi skal lykkes med å forvalte dette ansvaret må alle aktører som omfattes av dette politikkområdet være seg sitt ansvar bevisst. Aktører på alle nivåer må gjøre de nødvendige tiltak for å forebygge at det inntreffer uønskede hendelser og minske konsekvensene av de hendelsene som likevel inntreffer. En viktig del av det forbyggende arbeidet er å sikre tydelige ansvarslinjer og gjennomføre øvelser som følger av de råd som gis.

Styringsdokumentet er revidert i tråd med nye føringer for feltet etter 2019. Det gjelder først og fremst stortingsmelding Meld. St. 5 (2020-2021) *Samfunnssikkerhet i en usikker verden* og DSBs *Veileder til samfunnssikkerhetsinstruksen* (2019). Sikkerhetsloven som var helt ny da forrige utgave av styringsdokumentet ble publisert, har nå hatt tid til å virke en stund.

Samfunnsutviklingen og et endret trussel- og risikobilde gjør skillet mellom samfunnssikkerhet og statssikkerhet mer utydelig. Sikkerhetsloven reflekterer dette ved å omfatte nasjonal sikkerhet, som dekker statssikkerhet og deler av samfunnssikkerhetsområdet. Denne utgaven av styringsdokumentet omhandler også nasjonal sikkerhet og det forebyggende sikkerhetsarbeidet etter sikkerhetsloven.

Kunnskapsdepartementets politikkområde omfatter store deler av befolkningen, og virksomhetene i sektoren er svært forskjellige. Sektoren omfatter blant annet private og kommunale barnehager og skoler, stiftelser, statlige og private universiteter og høyskoler, aksjeselskaper, direktorater og andre forvaltningsorganer.

Styringsdokumentet inneholder krav og anbefalinger til departementets underliggende virksomheter, og anbefalinger for andre virksomheter. Målet med dokumentet er å bidra til systematisk og god oppfølging av arbeidet med sikkerhet og beredskap i kunnskapssektoren. Formålet er å legge til rette for at drøyt 1,6 millioner barnehagebarn, elever, studenter og ansatte skal være trygge der de oppholder seg store deler av dagen.

Kunnskapsdepartementet takker for mange nyttige innspill underveis i revisjonsarbeidet.

Lykke til i dette viktige arbeidet!

Petter Skarheim

Departementsråd

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, blant annet for å ivareta ulike ansvarsområder som til enhver tid har vært underlagt KD. Når dokumentet nå revideres på nytt er hovedmålene å tydeliggjøre hva som er krav og anbefalinger overfor virksomhetene i sektoren, samt å reflektere det stadig mindre tydelige skillet mellom samfunnssikkerhet og statssikkerhet. Overlapp og sammenhenger mellom ulike sikkerhetsområder har også bidratt til at dokumentet nå endrer navn. Dokumentet går med det fra å hovedsakelig vektlegge arbeidet med samfunnssikkerhet, til å omfatte de tre sikkerhetsområdene samfunnssikkerhet, nasjonal sikkerhet og informasjonssikkerhet og personvern. Inndelingen i ulike sikkerhetsområder har til hensikt å strukturere sikkerhetsarbeidet, som møter ulike krav i ulike regelverk. Samtidig legger KD til grunn at sikkerhetsarbeidet i sektoren følger en helhetlig tilnærming.

Veilederen for ROS-analyser som tidligere lå vedlagt, er nå tatt ut. Råd for samfunnssikkerhet og beredskap i kunnskapssektoren (Beredskapsrådet) jobber med en ny veileder.

Samfunnssikkerhetsinstruksen[1] understreker departementenes ansvar for samfunnssikkerhet i egen sektor og forklarer at "sektor" i denne sammenheng er departementets 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.

Styringsdokumentets relevans og anvendelse 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 og tildelingsbrev til departementets underliggende virksomheter, og den årlige budsjettproposisjonen (Prop. 1S).

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

2 Begreper og sammenhenger i arbeidet med sikkerhet og beredskap

Sentrale begreper i sikkerhets- og beredskapsarbeidet:

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.

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 statssikkerhet og en avgrenset del av samfunnssikkerhetsområdet, som er av vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser.

Nasjonale sikkerhetsinteresser er 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.[2]

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.[3]

Beredskap er definert som planlagte og forberedte tiltak som gjør oss i stand til å håndtere uønskede hendelser slik at konsekvensene blir minst mulig.

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

Krisehåndtering er summen av tiltak som iverksettes når en krise har inntruffet, for å begrense skadene og bringe krisen til opphør.

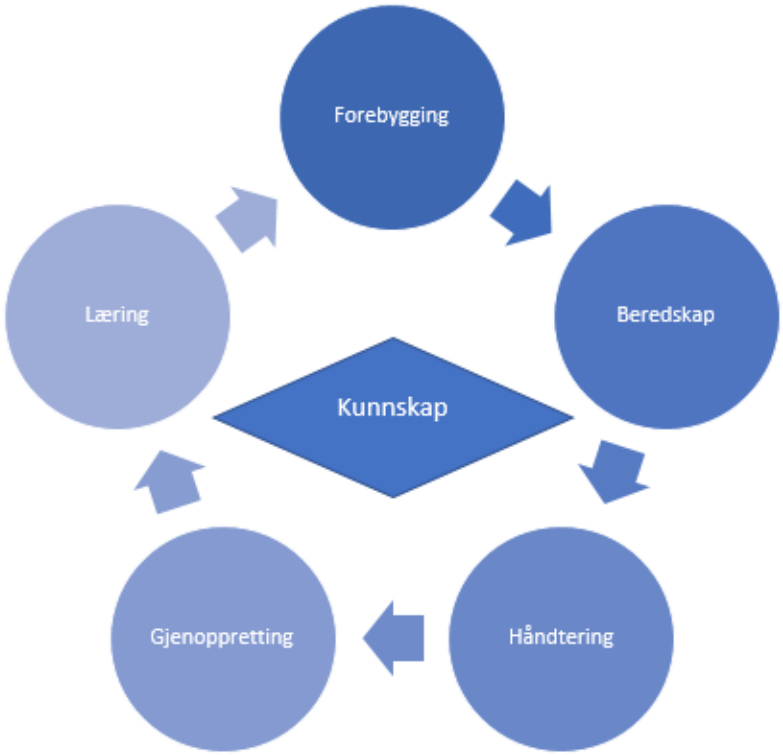
---

[2] Sikkerhetsloven § 1-5, punkt 1.

[3] Sikkerhetsloven § 1-5, punkt 3.

Sektor er innenfor samfunnssikkerhetsarbeidet 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 aktører som kommuner og private virksomheter.[4]

Definisjonene over er i stor grad hentet fra Meld. St. 5 (2020-2021) *Samfunnssikkerhet i en usikker verden*. 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.



Figur 1 Samfunnssikkerhet som en kjede[5]

Regjeringen ser arbeidet med samfunnssikkerhet som en kjede. Systematisk kunnskapsutvikling som grunnlag for forebyggende tiltak skal bidra til færre uønskede hendelser og et bedre beredskapsarbeid. God beredskap gjør ansvarlige aktører i stand til å håndtere hendelser og gjenopp-

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

[5] Figuren er hentet fra Meld. St. 5 (2020-2021): Samfunnssikkerhet i en usikker verden.

rette samfunnets funksjoner raskt, hvis hendelsen skulle inntreffe. I alle ledd av kjeden er kontinuerlig læring, forbedring og tilpasning til endringer i risiko- og sårbarhetsbildet en forutsetning for å lykkes.

3 Roller og ansvar, styringslinjer og virkemidler

3.1 Grunnleggende prinsipper for nasjonalt arbeid med samfunnssikkerhet

Samfunnssikkerhetsarbeidet tar utgangspunkt i verdiene vi skal beskytte, samfunnsfunksjoners sårbarheter, farene og truslene vi står overfor, samt vår evne til å forebygge og håndtere. I Norge baseres arbeidet med samfunnssikkerhet på fire grunnleggende prinsipper[6]:

Ansvarsprinsippet, som betyr at den organisasjonen som har et ansvar for et fagområde i en normalsituasjon, også har ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser på området.

Likhetsprinsippet, som betyr at den organisasjonen som skal håndtere en krise, i utgangspunktet er mest mulig lik den daglige organisasjonen.

Nærhetsprinsippet, som betyr at kriser organisatorisk skal håndteres på lavest mulig nivå.

Samvirkeprinsippet, som betyr at alle aktører har et selvstendig ansvar for å sikre optimalt samvirke og samarbeid med relevante aktører i arbeidet med forebygging, beredskap og krisehåndtering.

3.2 Sikkerhetskultur

Sikkerhet og beredskap handler først og fremst om mennesker. Summen av deres kunnskap, handlinger og holdninger til sikkerhet utgjør sikkerhetskulturen i en virksomhet. Alle virksomheter har en sikkerhetskultur. Hvor god den er, påvirker evnen til å styre sikkerheten og håndtere uønskede hendelser.

Det er et lederansvar å lage gode rammebetingelser og strukturer for arbeidet med sikkerhet og beredskap. Det er også ledernes ansvar å motivere medarbeidere til å handle på måter som ivaretar sikkerhet og styrker beredskap. Medarbeidere må vite hva som forventes av dem og forstå hvorfor sikkerhetstiltak eksisterer. Det krever opplæring. Medarbeiderne må også ansvarliggjøres, og samtidig gis trygghet til å melde fra om sikkerhetsmessige forhold som virksomheten bør vite om. Det forutsetter at ledere går foran som gode eksempler. På den måten kan virksomheten skape god sikkerhetskultur. God sikkerhetskultur kjennetegnes av at virksomhetens sikkerhetstiltak ivaretas av ledere og medarbeidere, sikkerhetstruende hendelser rapporteres og læring prioriteres.

[6] Samfunnssikkerhetsinstruksen kapittel III.

Forsvarlig sikkerhet og beredskap krever velfungerende samvirke på tvers av aktører og sektorer. Det forutsetter respekt for hverandres roller og ansvar, og ikke minst forståelse for at ulike aktører har ulike oppgaver og perspektiver som må hensyntas og veies opp mot hverandre.

Kriser kommer ofte overraskende. Krisehåndtering krever mer av ledere og medarbeidere enn oppgaveløsning i daglig drift. Vurderinger og beslutninger gjøres under større tidspress og med større usikkerhet enn i det daglige. Dessuten kan konsekvensene av feil beslutninger være større. Gode beslutninger under en krise forutsetter erfaring, høy kompetanse og et godt forebyggings- og beredskapsarbeid. Avklarte ansvarsforhold, god rolleforståelse og gjennomtenkte rutiner er spesielt viktig når hendelsene blir store. Det er avgjørende å vite hvem som har ansvar for hvilke oppgaver, og forstå hva dette betyr i ulike situasjoner. God rolleforståelse skapes gjennom praktisk erfaring, trening og øvelser.

3.3 Kunnskapsdepartementets sektoransvar for sikkerhet og beredskap

Samfunnssikkerhetsinstruksen fastslår at det enkelte departement har ansvar for samfunnssikkerhet i egen sektor. Dette 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. Det er den enkelte virksomhet som har det operative ansvaret for å ivareta samfunnssikkerheten ved egen virksomhet. Det følger av ansvars- og nærhetsprinsippet.

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 risiko- og sårbarhetsanalyser (ROS-analyser) med grunnlag i vurderinger av hendelser som kan true departementets 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 krisehåndtering 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 øvd. Se kap. 5.2 for mer om etablering av varslingsrutiner mellom virksomhetene og departementet.

Krisehåndteringen i KD ledes administrativt, av embetsverket. Den politiske ledelsen skal til enhver tid være godt orientert om hendelsesforløpet ved en krise.

For å kunne følge opp kravene i instruksen, må departementet avklare og beskrive departementets politikkområde når det gjelder samfunnssikkerhet. Herunder må roller, ansvarsområder og oppgaver som har betydning for å ivareta samfunnssikkerheten beskrives. Styringsdokumentet bidrar til å dokumentere dette.

KD har ikke hovedansvar for samfunnskritiske funksjoner, slik disse er definert av JD og Direktoratet for samfunnssikkerhet og beredskap (DSB).[7] Samtidig har KD et omfattende ansvar innen samfunnssikkerheten. Sektoren omfatter store deler av befolkningen og består 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, folkehøyskolene, 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. 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 forskningsdata, samlinger og historiske bygninger.

Oppsummert har KD ansvaret for følgende områder:

- Barnehager
- Det 13-årige utdanningsløpet fra grunnskolen til og med videregående opplæring
- Folkehøyskoler
- Høyere utdanning og 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

[7] DSB (2016): Samfunnets kritiske funksjoner.

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 samfunnssikkerhet. Overfor de øvrige delene av sektoren, herunder hele barnehage- og skolesektoren, har departementet kun 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.

For enkelte virksomhetstyper og aktiviteter er det særlig krevende å definere hva sektoransvaret innebærer. Det gjelder først og fremst statlig eide aksjeselskaper, der blant annet aksjeloven beskriver rolledeling mellom eier, styre og administrasjon, og virksomheter og aktivitet i utlandet.

Aksjeselskaper

Statsaksjeselskaper er aksjeselskaper der staten eier 100 prosent av aksjene. KD forvalter per 1.1. 2022 det statlige eierskapet i to statsaksjeselskaper: Simula Research Laboratory AS og Universitetssenteret på Svalbard AS (UNIS). I tillegg har de statlige universitetene og høyskolene ulikt eierskap 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 samfunnssikkerhet, slik dette er definert tidligere i dokumentet, men departementet har i hovedsak pedagogiske virkemidler til rådighet. 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.

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 sivile 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 elever og studenters sikkerhet i ut-

landet. 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. Se for øvrig 5.2 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 Kunnskapsdepartementets styringsvirkemidler

Departementets styringsvirkemidler kan deles inn i følgende hovedgrupper (som i praksis ikke trenger å være klart atskilt fra hverandre): juridiske, økonomiske, organisatoriske og pedagogiske. Nedenfor følger en gjennomgang av hvordan departementet kan benytte ulike virkemidler overfor ulike deler av sektoren. I tillegg kommer eierstyring av heleide aksjeselskaper og selskaper der departementet har dominerende eierinnflytelse.

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 således 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 miljørettet helsevern i barnehager og skoler som er en del av Helse- og omsorgsdepartementets (HODs) regelverk.[8] 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.

Veiledere i beredskapsarbeid er tilgjengelig på udir.no, dsb.no og sikresiden.no.

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

[8] Helse og omsorgsdepartementet (1996): Forskrift om miljørettet helsevern i barnehager og skoler mv.

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.

Skolenes arbeid med beredskap er regulert i forskrift om miljørettet helsevern i barnehager og skoler, 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.

Veiledere i beredskapsarbeid er tilgjengelig på udir.no, dsb.no og sikresiden.no.

Høyere yrkesfaglig utdanning

Fagskolene er enten private eller underlagt fylkeskommunene. Unntaket er Norges grønne fagskole (VEA) som er statlig underlagt KD, og som dermed følger 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.

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

Overfor alle disse virksomhetene er de pedagogiske virkemidlene, i form av veiledninger, møteplasser mv. viktige. Se Beredskapsrådet, udir.no, dsb.no og sikresiden.no for gode råd og veiledning.

Se for øvrig også avsnitt 12.3 om Beredskapsrådet, der fagskolene er representert.

Universiteter og høyskoler

De statlige høyere utdanningsinstitusjonene er virksomheter med egne styrer med særskilte fullmakter direkte underlagt KD. Dette medfører at KD har et særskilt ansvar for beredskapen ved disse virksomhetene. Departementet benytter ulike virkemidler i styringen av samfunnssikkerhetsarbeidet ved disse institusjonene og har instruksjonsmyndighet overfor disse. Mer om hva departementet konkret krever av disse virksomhetene følger i kapittel 7.

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

Også overfor denne gruppen virksomheter er de pedagogiske virkemidlene, i form av veiledninger, møteplasser mv. viktige. Se Beredskapsrådet, udir.no, dsb.no og sikresiden.no for gode råd og veiledning.

Se for øvrig også avsnitt 12.3 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 samfunnssikkerhet. Departementet oppfordrer like fullt studentsamskipnadene til å arbeide systematisk med samfunnssikkerhet i tråd med anbefalingene i styringsdokumentet.

Også overfor samskipnadene er de pedagogiske virkemidlene, i form av veiledninger, møteplasser mv. viktige. Se Beredskapsrådet, udir.no, dsb.no og sikresiden.no for gode råd og veiledning.

Se for øvrig også avsnitt 12.3 om Beredskapsrådet, der studentsamskipnadene er representert.

Folkehøgskoler

Hovedandelen av folkehøgskolene har privat eierskap, mens noen få er fylkeskommunalt/kommunalt eide. Folkehøyskolelovens regulering 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.

KD stiller ikke direkte krav til folkehøgskolenes arbeid med samfunnssikkerhet, men anbefaler at det tas utgangspunkt i veiledningene om beredskapsarbeid som er tilgjengelig på Udirs nettsider. Se udir.no, dsb.no og sikresiden.no for gode råd og veiledning.

Se for øvrig avsnitt 12.3 om Beredskapsrådet for UH-sektoren, der folkehøgskolene er representert.

Øvrige underliggende virksomheter

I tillegg til de høyere utdanningsinstitusjonene, har KD en rekke underliggende virksomheter av ulik størrelse, mandat og oppgaver. Se regjeringen.no for liste over de virksomhetene som til enhver tid er underlagt KD. KD har særskilt ansvar for samfunnssikkerheten ved disse virksomhetene. Departementet benytter ulike former for virkemidler i styringen av samfunnssikkerhetsarbeidet ved disse virksomhetene og har instruksjonsmyndighet overfor dem. Mer om hva departementet krever av disse virksomhetene følger i kapittel 3.5.

3.5 Kunnskapsdepartementets oppfølging av underliggende virksomheter

Nedenfor følger en beskrivelse av hvilke virkemidler KD bruker i styringen av samfunnssikkerhetsarbeidet ved *underliggende virksomheter*. Departementet vil tilpasse virkemiddelbruken til hva som til enhver tid er hensiktsmessig.

Fastsettelse av mål for arbeidet med sikkerhet og beredskap

Samfunnssikkerhetsinstruksen understreker at mål og prioriteringer innen samfunnssikkerhet skal gå fram av departementenes budsjettproposisjoner (Prop. 1 S) og at departementene gjennom etatsstyringen forsikrer seg om at de underliggende virksomhetene ivaretar samfunnssikkerheten på en systematisk måte.

Siden budsjettåret 2013-2014 har KDs budsjettproposisjon hatt en omtale av samfunnssikkerhetsarbeidet der det både rapporteres på spesielt viktige tiltak og orienteres om mål og prioriteringer.

Målsettinger og resultatoppfølging for samfunnssikkerhetsarbeidet har dessuten siden 2011 vært integrert i tidligere versjoner av dette styringsdokumentet. Styringsdokumentet er det viktigste virkemiddelet for å formidle krav som er konstante over en lengre tidsperiode. Med denne utgaven utvides målsettinger og resultatoppfølging til det forebyggende sikkerhetsarbeidet innen nasjonal sikkerhet, og til informasjonssikkerhet og personvern.

Ordinær styringsdialog

KD følger opp spørsmål knyttet til sikkerhet og beredskap blant annet gjennom tildelingsbrev, etatsstyringsmøter og brev med tilbakemelding i tilknytning til den årlige etatsstyringen og kontroller. Virksomhetenes økonomi- og virksomhetsinstrukser benyttes også for å understreke virksomhetenes ansvar på dette feltet. I tillegg er dette styringsdokumentet et viktig virkemiddel i styringsdialogen rundt sikkerhet og beredskap. I noen tilfeller sendes egne brev med rapporteringskrav til virksomhetene.

Kontroll av arbeidet med sikkerhet og beredskap

Det gjennomføres kontroll av arbeidet med sikkerhet og beredskap ved den enkelte virksomhet. NOKUT har ansvar for kontroll av samfunnssikkerhetsarbeidet i virksomhetene i høyere utdannings- og forskningssektoren og rapporterer til departementet. Virksomhetene får skriftlig tilbakemelding med eventuelle konkrete oppfølgingspunkter.

KD har selv ansvar for tilsvarende kontroll av underliggende virksomheter utenfor høyere utdannings- og forskningssektoren. Som et ledd i dette gjennomfører departementet såkalte beredskapstilsyn med virksomhetene. Hyppigheten på tilsyn ved den enkelte virksomhet avhenger av kvaliteten på arbeidet med sikkerhet og beredskap og en vurdering av risiko og vesentlighet. Tilsynene gir anledning til å gå i dybden på arbeidet ved virksomhetene og hvordan virksomhetene og KD sammen kan bidra til å styrke sikkerhet og beredskap. I tilsynene vurderer departementet etterlevelse av regelverk, men er samtidig i stor grad veiledende. Tilsynsrapportene som utarbeides i etterkant av tilsynene inneholder konkrete vurderinger av tilstanden ved virksomhetene og gir tilbakemelding om eventuelle oppfølgingspunkter.

Innen nasjonal sikkerhet har Nasjonal sikkerhetsmyndighet (NSM) ansvaret for at det forebyggende sikkerhetsarbeidet i alle sektorer kontrolleres, og skal se til at det føres tilsyn med at virksomheter oppfyller krav som følger av sikkerhetsloven med forskrifter. Departementet kan tildele en eksisterende sektormyndighet ansvar med 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 tillitt til det forebyggende sikkerhetsarbeidet og bidra til å redusere sårbarheter i virksomhetene, i sektoren og nasjonalt.

3.6 Statsforvalteren

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

3.7 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.

4 Risiko- og sårbarhetsanalyse av kunnskapssektoren

Samfunnssikkerhetsinstruksen stiller krav til at departementet utarbeider og vedlikeholder systematiske risiko- og sårbarhetsanalyser av tilsiktede og utilsiktede hendelser som kan true departementets og sektorens funksjonsevne og sette liv, helse og materielle verdier i fare.[9] Analysen skal ta utgangspunkt i overordnede nasjonale planleggingsgrunnlag som krisescenarioer, oversikt over

[9] Samfunnssikkerhetsinstruksen kapittel IV, punkt 2.

kritiske samfunnsfunksjoner og andre strategiske dokumenter om risiko, trusler og sårbarhet. Analysen kan, der det er naturlig, bygge på analyser og vurderinger gjort av underliggende virksomheter. Kunnskapsdepartementet gjennomfører en helhetlig risiko- og sårbarhetsanalyse av sektoren (Sektor-ROS) med noen års mellomrom. Analysen som ble gjennomført i 2020 ble delt med KDs underliggende virksomheter, men er unntatt offentlighet. På bakgrunn av Sektor-ROS og en vurdering av mulige tiltak skal departementene vurdere, beslutte og gjennomføre tiltak slik at sårbarheter og svakheter blir redusert innenfor hele sektoren. Utover arbeidet med den helhetlige risiko- og sårbarhetsanalysen for sektoren vurderes enkeltstående scenarioer fortløpende.

Analysen tar for seg alvorlige farer og trusler som kan ramme sektoren og gir anbefalinger om hva som kan gjøres for å redusere den risiko som foreligger. Analysen viser at sektoren kan bli rammet av svært ulike typer hendelser, ofte preget av at det er store samlinger av mennesker på avgrensede områder.

Sektor-ROS 2020 tar for seg scenarioer innenfor blant annet smittsomme sykdommer, ulykker, vold, terror og digitale hendelser. Analysen tok utgangspunkt i de 25 krisescenarioene som i 2019 forelå fra DSB.[10] Det ble vurdert hvordan disse eller lignende scenarioer ville kunne ramme kunnskapssektoren. ROS-analyser fra underliggende virksomheter og kommuner samt nasjonale trusselvurderinger bidro med ytterligere scenarioer for analysen. Totalt har analysen tatt for seg 20 scenarioer.

Nedenfor redegjør vi for fire av scenariene som var inkludert i KDs Sektor-ROS 2020; *skoleskyting, pandemi*, *digitale angrep og sammensatte trusler*. Dette er scenarioer som vurderes til høy risiko i Sektor-ROS. De trekkes frem her som aktuelle scenarioer som også virksomhetene i sektoren *kan* vurdere å inkludere i sine ROS-analyser. Relevansen av de fire scenarioene vil variere mellom virksomhetene.

I den grad det nevnes krav i dette kapittelet vises det til kapittel 5 om grunnleggende tiltak og kapittel 6 om informasjonssikkerhet der kravene (og anbefalinger) forklares nærmere.

4.1 Skoleskyting

Både KD i Sektor-ROS 2020 og DSB beskriver skoleskyting[11] som et scenario som det norske samfunnet bør planlegge for. Scenarioet vurderes til å medføre store konsekvenser. KD vurderte ikke sannsynlighet av tilsiktede hendelser i Sektor-ROS for 2020.

KD gjorde sin egen analyse av et slikt scenario i 2015 og denne analysen ble tatt med inn i Sektor-ROS 2020. Analysen bygde på DSBs krisescenario *terrorangrep i by*. Senere samme år utarbeidet DSB et scenario rundt en fiktiv skoleskyting ved en videregående skole på et tettsted i Nordland.

[10] DSB (2019): Analyser av krisescenarioer 2019.

[11] Begrepet skoleskyting er benyttet i styringsdokumentet som en oppfølging av Sektor-ROS 2020, og DSBs rapport, men det understrekes at begrepet i mange sammenhenger er erstattet av betegnelsen PLIVO (pågående livstruende vold) som favner ulike typer angrep.

DSBs risikoanalyse av skoleskyting er basert på informasjon fra forskning, granskingsrapporter og medieomtale av skoleskytinger i andre land. Representanter fra departementer, direktorater og lokale myndigheter har bidratt i arbeidet. Analysen tar for seg bakgrunn, drivkrefter og kontekst for skoleskyting og konkluderer med at forutsetningene for skoleskyting er til stede også i Norge.

DSB peker på at systematisk arbeid med et inkluderende læringsmiljø, forebygging mot mobbing, gode psykososiale tjenester og samarbeid om lokale beredskapsplaner, er med på å redusere risikoen for skoleskyting her i landet.

DSB trekker frem fem viktige tiltak for å forebygge skoleskyting. Dette er tiltak identifisert av DSB. KD mener at de må leses som sterke anbefalinger, men de er ikke krav til virksomheter i sektoren:

- Forebygge utenforskap
- Koordinering av instansene som er involvert i forebyggende arbeid og oppfølging av den enkelte elev (skolen, skolehelsetjenesten, kommunehelsetjenesten, politiet, barnevernet m.fl.)
- Beredskapsplan for skoleskyting ved den enkelte skole, og den må øves
- Lærere, skolehelsetjeneste og andre relevante aktører må ha nødvendig kunnskap om skoleskyting og den typiske gjerningspersonen
- Bygningsmessige tiltak (talevarslingsanlegg, rømningsmuligheter)

I Sektor-ROS 2020 er det utarbeidet flere scenarioer innunder kategoriene *politisk motivert vold* og *hevnmotivert vold*. Hendelser innenfor disse kategoriene kan ramme de ulike delene av KDs sektor.

Departementet forventer at høyere utdanningsinstitusjoner regelmessig vurderer egne beredskapsplaner og gjennomfører øvelser knyttet til alvorlige hendelser. Se mer om dette i kapittel 5.

KD legger til grunn at kommunen og skoleledelsen regelmessig vurderer om egne beredskapsplaner, både på kommunalt nivå og skolens nivå, i tilstrekkelig grad dekker alvorlige tilsiktede hendelser som skoleskyting. Øvelser må gjennomføres på en måte som ivaretar skolens behov for å være forberedt på en alvorlig hendelse, men uten å virke skremmende på elevene.

4.2 Pandemi

KD har i Sektor-ROS vurdert hvordan en pandemi kan ramme egen sektor. Covid-19-pandemien har påvirket KDs sektor i stor grad. Pandemien har samtidig gitt både departementet og virksomhetene i sektoren svært verdifull erfaring med krisehåndtering, men også forebyggende arbeid og beredskapsarbeid. Pandemi er blant de av DSBs krisescenarioer som kommer høyest opp i risikomatrisen, hvor det vurderes til høy risiko, med høy sannsynlighet og svært store samfunnsmessige konsekvenser. En alvorlig pandemi er dermed en av de største utfordringene for samfunnssikkerheten.

Nasjonal beredskapsplan for pandemisk influensa (Helse- og omsorgsdepartementet 2014) fastslår at det er viktig at både helsetjenesten og andre samfunnssektorer er godt forberedt på å kunne håndtere en influensapandemi. Den nasjonale beredskapsplanen skal sikre felles nasjonal planlegging og håndtering av en pandemi. Beredskapsplanen fastsetter ansvar og fordeler oppgaver for håndteringen på en rekke instanser, både i og utenfor helsetjenesten. Det er et mål at man under

en pandemi skal kunne opprettholde nødvendige samfunnsfunksjoner innen alle samfunnssektorer så langt det er mulig. Alle sektorer må være forberedt på en pandemi med høyt sykefravær. Den nasjonale beredskapsplanen revideres høsten 2021.

Barnehage- og skolebarn samt ansatte i barnehager/skoler er utsatte grupper ved en eventuell pandemi. I flere pandemier har barn blitt lett smittet, og i barnehager/skoler/SFO er mange barn samlet. Myndigheten til å stenge institusjonene ligger iht. smittevernloven hos den enkelte kommune (gjelder også private barnehager/skoler). Helsemyndighetene kan fatte vedtak om stenging av slike institusjoner for hele eller deler av landet. Behovet for omfattende stenging må nøye avveies mot de store samfunnsmessige ringvirkningene dersom mange friske arbeidstakere må være hjemme med friske barn på grunn av stengte barnehager, skoler eller SFO.

Skole- og barnehageeier skal påse at virksomheten har etablert et system for best mulig å forebygge sykdom og har ansvar for at de ansatte gis relevant og tilstrekkelig opplæring i dette. Leder i skole og barnehage er ansvarlig for at elever og barn vernes mot eventuelle helseskader og for å iverksette de tiltak som er nødvendig (forskrift om miljørettet helsevern i barnehager og skoler). Stenging på grunn av sykdom blant personalet bør søkes unngått gjennom planlegging av gode vikarordninger.

KD stiller krav til at alle de underliggende virksomhetene i sektoren utarbeider en egen pandemiplan. Denne skal oppdateres ved behov slik at man er forberedt dersom et pandemiutbrudd skulle inntreffe. Se kap. 5 for mer om dette. KD forutsetter at også kommunene og private aktører gjennomgår og oppdaterer sine pandemiplaner ved behov. Se for øvrig også kap. 5 om krav til kontinuitetsplan for virksomhetene.

4.3 Digitale angrep

Sektor-ROS 2020 omfattet flere scenarioer med digitale angrep mot infrastruktur i KDs sektor. Scenarioene ble vurdert til fra middels til høy risiko med store konsekvenser. KD vurderte ikke sannsynlighet for tilsiktede hendelser.

Nasjonalt cybersikkerhetssenter (NCSC) i NSM observerer ulike typer digitale operasjoner mot norske mål, inkludert mot virksomheter som ivaretar viktige samfunnsfunksjoner. En gjennomgående erfaring er at digitale operasjoner blir mer sofistikerte og komplekse, og at hendelseshåndtering er tid- og ressurskrevende. En annen erfaring er at løsepengevirus i økende grad rammer norske virksomheter. NSM har i flere år rapportert om at det er kjente sårbarheter som benyttes for å gi uautorisert tilgang til systemer og nettverk. Det digitale risikobildet preges av dette.

NSM ser at målrettede og ikke-målrettede digitale angrep treffer bredere enn tiltenkt, og understreker at de som ikke har beskyttet seg må forvente å bli rammet. NSM, Politiets sikkerhetstjeneste (PST), Etterretningstjenesten og Kripos ser et jevnt trykk av nettverksbaserte etterretningsoperasjoner fra statlige eller statstilknyttede aktører mot norske myndigheter og virksomheter.

Behovet for åpenhet og internasjonalt samarbeid i akademiske miljøer innebærer sårbarhet for at fremmede etterretningstjenester kan utnytte blant annet legitimt forskningssamarbeid for å skaffe sensitiv informasjon og teknologi fra norsk forskning. Norske forsknings- og høykompetansemiljøer innen flere fagfelt er av stor interesse for fremmed etterretning. NSM anbefaler at myndigheter og

forskningsinstitusjoner samarbeider om bevisstgjøring og kompetanseheving om risiko knyttet til fremmed etterretning i forsknings-, utviklings- og teknologimiljøer.

I Units (nå HK-dir) Risiko- og tilstandsvurdering 2021 vurderes risikoen for skadevarehendelser, særlig større løsepengevirusangrep, som høy. Risikoen for kompromitterte kontoer (at en trusselaktør tar kontroll over brukerkontoer) vurderes også som høy, og i 2020 ble det rapportert om opp mot 300 tilfeller av kontoer på avveie.[12]

NSM erfarer at mange virksomheter fortsatt mangler kompetanse på gjennomføring av risikovurderinger.[13] NSM er av den oppfatning at norske virksomheter er bedre rustet mot uønskede digitale hendelser hvis de følger rådene i *NSMs Grunnprinsipper for IKT-sikkerhet,* jf. kap. 6.5.

KDs underliggende virksomheter skal ha planer for å forebygge, avdekke og håndtere cyberangrep og skal være tilknyttet ressursmiljøer som kan bistå i arbeidet. KD forutsetter at øvrige virksomheter i alle deler av sektoren gjør tilsvarende.

Se kapittel 6 – informasjonssikkerhet – for omtale av sentrale tiltak for å forebygge og håndtere cyberangrep.

4.4 Sammensatte trusler

Sammensatte trusler er en betegnelse på strategier for konkurranse og konfrontasjon under terskelen for væpnet konflikt. Ulike typer virkemidler brukes i kombinasjon for å nå strategiske målsettinger. Virkemidlene kan være åpne og fordekte, militære og ikke-militære, i det fysiske og i det digitale rom.[14] De ulike virkemidlene brukes gjerne bredt distribuert og med en langsiktig tilnærming. Sammensatte trusler kan fremstå som en utfordring for samfunnssikkerheten, men er rettet mot statssikkerheten. Det kan også være krevende å skille mellom legitime handlinger, utilsiktede effekter og en tilsiktet ondsinnet handling. Sammensatte trusler er i sin natur komplekse og gjenstridige problemer som utfordrer tidlig varsling, omforent situasjonsforståelse og samordnet håndtering.

Fenomenet er i prinsippet ikke noe nytt og eksempler på sammensatte trusler kan spores tilbake til antikken. Men dette er spesielt aktuelt i vår tid, fordi sammensatte truslers betydning ser ut til å øke relativt til militær maktanvendelse.

Et av virkemiddelene som knyttes til sammensatte trusler er påvirkningsoperasjoner. Her benyttes blant annet desinformasjon for å undergrave tillit eller påvirke politiske prosesser ved å forsterke konflikter, skape usikkerhet eller likegyldighet til sannhet og fakta. En påvirkningsoperasjon kan for

---

[12] Unit (2021): Informasjonssikkerhet og personvern i høyere utdanning og forskning - Risiko- og tilstandsvurdering 2021, s. 62, tilgjengelig på: https://www.unit.no/media/2687/download?inline

[13] NSM (2021): Risiko 2021, og Etterretningstjenesten (2021): Fokus 2021.

[14] JD/FD (2018): Støtte og samarbeid. En beskrivelse av totalforsvaret i dag.

eksempel være lekking av stjålet konfidensiell informasjon for å svekke verdier som akademisk frihet og åpenhet. Det kan også være digital mobbing eller utpressing for å hindre ytringer, eller for å få tilgang til forskning.

I Sektor-ROS 2020 analyserte KD et scenario rundt påvirkning av skoleelever forut for et skolevalg. De samlede konsekvensene ble vurdert til små, men det er mulig å se for seg at virksomheter og enkeltindivider innenfor KDs ansvarsområde kan bli utsatt for sammensatte trusler som kan få alvorlige konsekvenser. Barn og unge kan blant annet bli påvirket av målrettede cyberoperasjoner i sosiale medier som enten er rettet mot å skade kunnskapssektoren eller å skape uro og forvirring i samfunnet. Virksomhetene i sektoren bør ha en bevisst holdning til denne typen trusler, ikke minst er det viktig å se ulike hendelser eller aktiviteter i sammenheng.

DSBs krisescenario om legemiddelmangel viser et eksempel som kan knyttes til sammensatte trusler: Desinformasjon om knapphet på legemidler fører til hamstring som deretter skaper reell mangel på viktige legemidler.

5 Grunnleggende tiltak

Det er viktig at alle aktører i KDs sektor jobber systematisk og helhetlig med samfunnssikkerhet.

Det som omtales i dette kapittelet må regnes som krav til underliggende virksomheter og sterke anbefalinger til andre virksomheter i sektoren. Der det står "skal" må dette altså leses som "bør" for de virksomhetene som ikke er direkte underlagt departementet. Alle kravene i listen under skal dokumenteres skriftlig og dato for gjennomgang/revisjon må fremkomme.

KDs underliggende virksomheter skal/andre virksomheter i sektoren bør:
ROS-analyse • Utarbeide ROS-analyser som omfatter de tre sikkerhetsområdene samfunnssikkerhet og beredskap, nasjonal sikkerhet, og informasjonssikkerhet og personvern. • Analysen skal gjennomgås minimum hvert år og revideres ved behov. • Analysen skal presenteres i en helhetlig rapport. • Utarbeide en tiltaksplan til ROS-analysen for samtlige uønskede hendelser med middels eller høy risiko (denne kan inkluderes i den helhetlige ROS-rapporten). • Tiltaksplanen skal beskrive hvordan de enkelte tiltakene reduserer sannsynligheten for, og konsekvensene av, de uønskede hendelsene. **Krise- og beredskapsplaner** • Utarbeide en krise- og 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)
- Rutiner for koordinering med andre aktører

- Utarbeide en kontinuitetsplan som del av beredskapsplanen. Holdes oppdatert og revideres ved behov.
- Utarbeide en pandemiplan som utfyller beredskapsplanen. Revideres ved behov.

Krise- og beredskapsøvelser

- Gjennomføre minimum en krise- og beredskapsøvelse per år. Øvelsene skal ta utgangspunkt i uønskede hendelser identifisert i virksomhetens ROS-analyse.
- Utarbeide en årlig øvelsesplan som minimum skal inneholde:
  - Formålet med den enkelte øvelse
  - Tid og sted for gjennomføring
  - Øvelsesscenario
  - Type øvelse
  - Målgruppe
- Gjennomføre og dokumentere evalueringer av gjennomførte beredskapsøvelser og reelle hendelser.
- Gjennomføre ledelsesforankrede oppfølgingsplaner. Disse skal som et minimum inneholde:
  - Læringspunkter
  - Beskrivelse av tiltakene
  - Tidsramme/frist for gjennomføring av tiltakene
  - Ansvarlig for hvert enkelt tiltak

5.1 Risiko- og sårbarhetsanalyser

Målet med ROS-analyser er å identifisere uønskede hendelser som kan inntreffe, vurdere risiko og sårbarhet knyttet til hendelsene og utarbeide tiltak som er nødvendige 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 samfunnssikkerhets- og beredskapsarbeidet.

Arbeidet med ROS-analyser er en systematisk prosess som kan baseres på ulike fremgangsmåter og standarder, deriblant ISO 31000 (Risikostyring) og NS 5814 (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 sin egen situasjon og tilpasser analysene til hva som er relevant for denne. ROS-analysene skal være nyttige verktøy i det konkrete arbeidet med samfunnssikkerhet og beredskap.

Arbeidet med sikkerhet og beredskap skal være en integrert del av den helhetlige virksomhetsstyringen. Det er derfor hensiktsmessig å se ROS-analyser i sammenheng med virksomhetens øvrige risikoanalyser, deriblant av måloppnåelse og helse, miljø og sikkerhet (HMS). Å se disse i sammenheng kan for eksempel innebære at man gjør seg kjent med øvrige risikoanalyser, identifiserer hendelser som kan være relevante for flere av risikoanalysene, og bruker integrerbare kategoriinndelinger.

KD anbefaler at ROS-analysene som omfatter samfunnssikkerhet, nasjonal sikkerhet, og informasjonssikkerhet og personvern utarbeides separat fra HMS. Dette bidrar til at både HMS og de tre sikkerhetsområdene vies tilstrekkelig ressurser og fokus, og at analysene legges til grunn for videre planverk innenfor begge feltene. Det er likevel mulig å integrere analysene dersom man finner gode løsninger på dette, men dette krever at man er bevisst formålet med de ulike analysene og at disse legges til grunn for videre oppfølging innenfor de ulike områdene.

KD anbefaler at virksomhetene i sitt arbeid med ROS-analyser henter inspirasjon fra blant annet DSBs krisescenarioer og de årlige trusselvurderingene fra henholdsvis NSM, PST og Etterretningstjenesten 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.

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.

De to foregående utgavene av dette styringsdokumentet hadde et vedlegg med veiledning til arbeidet med ROS-analyser. Vedlegget er nå tatt ut, og Beredskapsrådet jobber med en ny veileder.

5.2 Krise- og 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 krise- og beredskapsplaner for håndtering av uønskede hendelser eller kriser. Planen skal utarbeides på grunnlag av ROS-analysen.

Krise- og beredskapsplanen må være lett tilgjengelig, og som et minimum inneholde:

- 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)
- Rutiner for koordinering med andre aktører

Jf. første kulepunkt kan tiltakskort som beskriver roller og ansvar være en hensiktsmessig del av beredskapsplanen.

Jf. tredje kulepunkt skal alle virksomheter ha etablerte rutiner for hvordan også departementet skal varsles ved en uønsket hendelse. Virksomhetene har ansvar for å holde departementet tilstrekkelig orientert ved en hendelse. I tillegg til varsling, innebærer dette også informasjonsdeling og rapportering.

Virksomhetene skal som en del av beredskapsplanen utarbeide en kontinuitetsplan for å opprettholde kritiske funksjoner ved høyt personellfravær, uavhengig av årsak. DSB har utarbeidet en veileder for kontinuitetsplanlegging som kan være nyttig å benytte.

I kapittel 4.2 beskrives pandemi som et 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 krise- og beredskapsplanverket, og revidere ved behov. Dette er særlig aktuelt i etterkant av øvelser og reelle hendelser der krise- og/eller hendelseshåndteringsevnen til virksomheten er prøvd ut.

5.3 Krise- og beredskapsøvelser

Øvelser er læringsarenaer som skal bidra til at ledere og medarbeidere i virksomheten kjenner krise- og 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. Øvelser og hendelser 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.

6 Informasjonssikkerhet og personvern

Informasjon behandles i et samspill mellom mennesker, prosesser og teknologi. Informasjonssikkerhet[15] handler om å sikre denne informasjonsbehandlingen og dermed verdiene som informasjon representerer. Det er ledelsen ved den enkelte virksomhet som har ansvaret for å etablere og opprettholde tilfredsstillende informasjonssikkerhet. Informasjonssikkerhet skal være en integrert

[15] Dette inkluderer sikkerhet i alle IKT-systemer, IKT-tjenester og IKT-komponenter som inngår i systemene. Informasjonssikkerhet omfatter «IKT-sikkerhet», «digital sikkerhet» og de fleste beskrivelser av «cybersikkerhet», og i tillegg også fysisk sikkerhet (fysisk sikring av informasjon og informasjonssystemer) og organisatorisk sikkerhet (herunder også lovmessig etterlevelse, styringssystemer, regelverk, prosesser, prosedyrer og avtaler).

del av det øvrige sikkerhetsarbeidet i virksomheten og skal inngå i den helhetlige virksomhetsstyringen.[16] I kapittel 7, om sikkerhetsloven, beskrives det hvordan arbeidet med informasjonssikkerhet, forebyggende sikkerhetsarbeid og virksomhetsstyring kan samordnes.

KD har økt oppmerksomhet om dette området som følge av et skjerpet digitalt risikobilde, og forventer at arbeidet med informasjonssikkerhet og personopplysningssikkerhet gis høy prioritet hos alle virksomhetene i sektoren.

Som i kapittel 7, 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 og personvern.

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.[17] 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.[18] Siste versjon av policyen er til enhver tid tilgjengelig på regjeringens nettsider under Kunnskapsdepartementets rundskriv. HK-dir har ansvar for den løpende sektorstyringen av arbeidet med informasjonssikkerhet og personvern i høyere utdanning og forskning, og skal følge opp at kravene i policyen etterleves. NOKUT fører uavhengig kontroll med etterlevelse av policyen. Sikt leverer viktige tjenester som skal styrke sikkerheten, i tråd med disse kravene.

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.

---

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

[17] De aktuelle virksomhetene er: statlige universiteter og høyskoler, direktoratene HK-dir, NOKUT og Sikt, Norges forskningsråd, aksjeselskapene UNIS og Simula, De nasjonale forskningsetiske komiteene og NUPI.

[18] 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.

Et viktig grunnlag for arbeidet med informasjonssikkerhet, både i KD og i virksomhetene i sektoren, er: Nasjonal strategi for digital sikkerhet, Nasjonal strategi for digital sikkerhetskompetanse, Digitaliseringsstrategi for grunnopplæringen med handlingsplan, Strategi for digital omstilling i universitets- og høyskolesektoren.

KDs underliggende virksomheter skal:
• Følge gjeldende regelverk, inkludert forvaltningsloven med e-forvaltningsforskriften, offentlighetsloven med forskrifter, sikkerhetsloven med forskrifter, personopplysningsloven med forskrifter, helseregisterloven med forskrifter, ekomloven med forskrifter, esignaturloven med forskrifter og reglement for økonomistyring i staten.
KDs underliggende virksomheter som er omfattet av KDs 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
KDs underliggende virksomheter skal/andre virksomheter i sektoren bør:
• Etablere et helhetlig ledelsessystem for informasjonssikkerhet

6.1 Risikostyring og ledelse av informasjonssikkerhet og personvern

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. Informasjonssikkerhet handler om å beskytte disse informasjonsverdiene.

De overordnede målene for informasjonssikkerhet er å ivareta 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.[19] I de tilfellene der informasjonssikkerheten kan ha konsekvenser for liv og helse er også fysisk sikkerhet et helt sentralt sikkerhetsmål.

Disse målene reflekteres også i krav til informasjonssikkerhet som er innlemmet i flere lover og forskrifter, inkludert forvaltningsloven med e-forvaltningsforskriften, offentlighetsloven med forskrifter, sikkerhetsloven med forskrifter, personopplysningsloven med forskrifter, helseregisterloven med forskrifter, ekomloven med forskrifter, esignaturloven med forskrifter og reglement for økonomistyring i staten. Lovverket stiller krav til forsvarlig informasjonsbehandling og riktig beskyttelsesnivå, noe som blir særlig gjeldende i møte med økt digitalisering.

Digitalt sårbarhetsutvalg (Lysneutvalget) viste tidlig til at Norge har ligget langt fremme når det gjelder digitalisering, noe som gjør at vi som samfunn også tidlig har møtt sårbarhetsutfordringer.[20] Flere viktige systemer har blitt koblet på nett, og inngangsportene for en angriper er i dag mange. Leverandørkjeder kan bli lange og krevende å følge opp. Digitale avhengigheter har fått komplekse sammenhenger, og medfører nye sårbarheter.[21] 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. Dette øker robusthet, men også bevissthet og forståelse for sikkerhet hos den enkelte.[22]

Tiltaksområdene omfatter både menneskelige, tekniske og organisatoriske aktiviteter og investeringer, innenfor både IKT-infrastrukturen, forsvarlig informasjonsbehandling og arbeidsprosesser, og robuste responsmiljø. Det er nødvendig å bygge en sikkerhetskultur hvor oppmerksomhet og

---

[19] 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.

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

[21] DSB (2020): Risikostyring i digitale verdikjeder, tilgjengelig på: https://www.dsb.no/globalassets/dokumenter/rapporter/risikostyring-i-digitale-verdikjeder.pdf

[22] NSM (2021): Nasjonalt digitalt risikobilde 2021, tilgjengelig på: https://nsm.no/aktuelt/nasjonalt-digitalt-risikobilde-2021

kunnskap om informasjonssikkerhet er en del av den strategiske organisasjonsutviklingen. Informasjonssikkerhet og personvern favner dermed bredt, og må sees på som et viktig internkontrollområde og et ansvar som strekker seg ut over virksomhetens IT-avdeling.

Alle KDs underliggende virksomheter skal ha et helhetlig ledelsessystem for informasjonssikkerhet. 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 at det er nok ressurser til å støtte et tilfredsstillende arbeid med informasjonssikkerhet og personvern i virksomheten.

6.2 Håndtering av hendelser

Håndtering av alvorlige informasjonssikkerhetsbrudd og personvernhendelser inngår i ledelsessystemet for informasjonssikkerhet og internkontrollen for personvern. Alle virksomheter må ha en beredskapsplan for å kunne håndtere de hendelsene som kan inntreffe (se også kap. 5.2). 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 fjerne årsakene til informasjonssikkerhetsbrudd og personvernhendelser. Det skal også bidra til at virksomhetene kan videreføre kritiske oppgaver samtidig som håndtering av hendelser og gjenoppretting av normal drift pågår. Utdanningsinstitusjonenes håndtering av Covid 19-situasjonen er et eksempel på at evnen til å gjennomføre viktige deler av samfunnsoppdraget under vanskelige og unormale omstendigheter, for eksempel undervisning og eksamensavvikling, har stor verdi for studenter og ansatte.[23]

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 (jf. Lysneutvalgets NOU 2015:13). 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.

[23] Unit (2020): Kontinuitet, beredskap og øvelser, tilgjengelig på: https://www.unit.no/media/2048/download?attachment

KD har innført dette rammeverket for virksomhetene som er omfattet av KDs styringsmodell for informasjonssikkerhet og personvern i høyere utdanning og forskning.[24] Cybersikkerhetssenter for forskning og utdanning (tidligere Uninett CERT) er utpekt som sektorvist responsmiljø for virksomheter underlagt rammeverket. Disse virksomhetene har egne lokale responsteam, og et tett samarbeid med sektorvist responsmiljø gjør at disse nå er bedre forberedt til å håndtere fremtidige trusler og hendelser. Departementet er i gang med prosesser for å beslutte om rammeverket også skal gjøres gjeldende for de øvrige virksomhetene underlagt KD.

6.3 Forsvarlig behandling av personopplysninger

> *Personvern dreier seg om ivaretakelse av personlig integritet; ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse.*[25]

Personvern og informasjonssikkerhet er et kontinuerlig arbeid, og må derfor gis løpende oppmerksomhet. Endringer i systemer og rutiner kan få konsekvenser for virksomhetens evne til å behandle personopplysninger på en god måte. Personvern og informasjonssikkerhet handler om kultur og bevissthet. Det er derfor viktig at ledelsen tar ansvar og gir arbeidet med personvern og informasjonssikkerhet prioritet.

Informasjonssikkerhet dreier seg om å håndtere risikoen for at personopplysninger og andre informasjonsverdier 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.[26]

Artikkel 5 i GDPR stiller krav om overholdelse av personvernprinsippene:

- Prinsippet om lovlighet, rettferdighet og åpenhet: Personopplysninger skal behandles på en lovlig, rettferdig og gjennomsiktig måte. Behandlingen skal ha et rettslig grunnlag, og de registrertes rettigheter skal ivaretas.
- Prinsippet om formålsbegrensning: Personopplysninger skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles på en måte som er uforenlig med disse formålene.
- Prinsippet om dataminimering: Personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for.

---

[24] Unit (2020): Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren, tilgjengelig på: https://www.unit.no/rammeverk-handtering-av-ikt-sikkerhetshendelser-i-uh-sektoren

[25] Fornyings- og administrasjonsdepartementet (2009): NOU 2009: 1 - Individ og integritet – Personvern i det digitale samfunnet, tilgjengelig på: https://www.regjeringen.no/no/dokumenter/nou-2009-1/id542049/

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

- Prinsippet om opplysningskvalitet: Personopplysningene skal være korrekte og oppdaterte.
- Prinsippet om lagringsbegrensning: Personopplysningene skal ikke lagres lenger enn det som er nødvendig for å oppfylle formålet som personopplysningene behandles for.
- Prinsippet om integritet og konfidensialitet: Hensynet til integritet og konfidensialitet skal ivaretas ved behandlingen. Personopplysningene skal behandles på en sikker måte, ved bruk av egnede tekniske eller organisatoriske tiltak.
- Prinsippet om ansvarlighet: Virksomhetene skal kunne dokumentere at de ovennevnte personvernprinsippene blir overholdt ved behandling av personopplysninger.

All behandling av personopplysninger forutsetter tilpassede informasjonssikkerhetstiltak. Dette er et viktig, men ikke nødvendigvis tilstrekkelig element i godt personvern. Regelverket forutsetter at sikringstiltakene er 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. Dette gjøres ved å etablere og vedlikeholde tiltak for å sikre at personopplysningene behandles i samsvar med regelverket, ved å etablere internkontroll. Virksomhetene har varslingsplikt til Datatilsynet og den registrerte ved brudd på personopplysningssikkerheten.

KD legger til grunn at virksomhetene i kunnskapssektoren er bevisst det ansvaret som påligger den enkelte virksomhet i etterlevelse av personvernlovgivningen.

6.4 Særlig om tjenesteutsetting

Det må gjøres særskilte vurderinger når en skal sette ut tjenester til eksterne leverandører, som for eksempel ved bruk av skytjenester.[27] 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. Formålet er å sikre at personopplysningsvernet blir det samme ved overføring til stater som ikke har det samme beskyttelsesnivået, som innenfor EØS-området. Det er viktig at virksomheten vurderer om overføringsgrunnlaget faktisk vil fungere slik det skal i forkant av en behandling. Hvis overføringsgrunnlaget ikke sikrer god nok beskyttelse for personopplysningene i seg selv, må man i tillegg iverksette andre tiltak.[28]

Overføring av personopplysninger til USA kunne tidligere skje dersom mottakeren var sertifisert etter EU-US Privacy Shield-rammeverket. Denne avtalen ble kjent ugyldig av EU-kommisjonen i den

[27] NOU 2015: 13 - Digital sårbarhet – sikkert samfunn.

[28] 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/

såkalte Schrems II-dommen 16.7.20. Dette innebærer at overføringer til USA må baseres på andre overføringsgrunnlag, jf. personvernforordningen kapittel V. Det er derfor særlig grunn for virksomhetene til å gå gjennom sine avtaler med tjenesteleverandører («tilbydere av elektroniske kommunikasjonstjenester») for å sikre at behandling av personopplysninger er i henhold til gjeldende regelverk.

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. Nasjonalt ressurssenter for deling av data/Digitaliseringsdirektoratet leder i tillegg et koordineringsarbeid med offentlige virksomheter, der formålet er å utveksle erfaringer og veilede offentlige virksomheter om tiltak og tilnærming til utfordringene som følge av Schrems II-dommen.

6.5 Råd og anbefalinger for å styrke informasjonssikkerhet og personvern

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 implementere 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.

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.

I forbindelse med sitt ansvar for den løpende sektorstyringen i UH-sektoren gjennomfører Direktoratet for høyere utdanning og kompetanse (HK-dir) årlige kartlegginger av arbeidet med informasjonssikkerhet og personvern hos den enkelte virksomhet. På bakgrunn av dette mottar 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. Virksomhetene kan benytte rapporten 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 til grunn for sin egen risikostyring på informasjonssikkerhets- og personvernområdet.

Cybersikkerhetssenteret for forskning og utdanning ble etablert i 2021. Uninett (Sikt, etter 2021) er ansvarlig for arbeidet, og utfører dette i tett samarbeid med UiO, NTNU og Norsk Senter for Forskningsdata (Sikt, etter 2021). 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*. I arbeidet til senteret ligger også de oppgaver som er tilknyttet rollen som «sektorvist responsmiljø», i henhold til *Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren*. Cybersikkerhetssenteret vurderer sektorfellesskapet som den viktigste verdien for å skape økt beskyttelse og robusthet mot cybertrusselen, både på sektornivå og for hver virksomhet.

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 og personvern som utvikles og tilgjengeliggjøres gjennom Sikresiden.no. Digitaliseringsdirektoratet har 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. 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 og personvern. I tillegg inneholder Utdanningsdirektoratets nettsider om sikkerhet og beredskap nyttig informasjon om personvern i barnehage og skole.

I arbeidet med sikkerhetskultur og opplæring anbefaler KD at universiteter og høgskoler benytter seg av de kurs og opplæringstilbud som Cybersikkerhetssenteret tilbyr.

7 Sikkerhetsloven

Alle KDs underliggende virksomheter omfattes av sikkerhetsloven. Loven skal bidra til å trygge nasjonale sikkerhetsinteresser ved å forebygge, avdekke og motvirke sikkerhetstruende virksomhet.

Den 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, samt leverandører av varer og tjenester i forbindelse med en sikkerhetsgradert anskaffelse. I tillegg kan departementet innenfor sitt ansvarsområde fatte vedtak om å helt eller delvis underlegge andre virksomheter.

Under følger en oversikt over kravene som stilles i dette kapittelet.

Alle virksomheter i sektoren som er underlagt sikkerhetsloven skal:

Styringssystem for sikkerhet

- Utarbeide styringssystem or sikkerhet som skal omfatte:
  - Risikostyring
  - Sikkerhetsledelse
  - Sikkerhetsorganisering
  - Sikkerhetstiltak- og prosedyrer
  - Forholdet til andre virksomheter
  - Sikkerhetsoppfølging
  - Sikkerhetsdokumentasjon
- Samordne styringssystemet med ledelsessystem for informasjonssikkerhet og virksomhetsstyringen.
- Dokumentere styringssystemet skriftlig og revidere ved behov.

Skjermingsverdige verdier

- Vurdere, kartlegge og holde oversikt over virksomhetens skjermingsverdige verdier (definert som skjermingsverdig informasjon, informasjonssystemer, infrastruktur eller objekter).[30]

Sikkerhetsklarerte og autoriserte

- Føre oversikt over virksomhetens ansatte som er sikkerhetsklarert og/eller autorisert iht. sikkerhetsloven. Oversikten skal til enhver tid være oppdatert.

[29] Sikkerhetsloven § 1-1.

[30] Virksomhetssikkerhetsforskriften § 2.

7.1 Styringssystem for sikkerhet

Alle virksomheter som omfattes av sikkerhetsloven skal ha et dokumentert styringssystem for sikkerhet.[31] 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 skal derfor dekke:

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

Styringssystemet skal bidra til at virksomheten oppfyller kravene gitt i eller med hjemmel i loven. Utformingen av styringssystemet må tilpasses verdiene som skal beskyttes og måten de beskyttes på. Det må dimensjoneres i forhold til risiko for sikkerhetstruende virksomhet. Hva som er riktig utforming og dimensjonering for å oppnå og opprettholde et forsvarlig sikkerhetsnivå vil variere fra en virksomhet til en annen. Styringssystemet vil derfor være utformet og dimensjonert ulikt i sektorens ulike virksomheter.

Styringssystemet skal være utformet helhetlig og samordnet med ledelsessystem for informasjonssikkerhet og personvern og virksomhetsstyringen for øvrig. Det gir grunnlag for felles tilnærming i håndteringen av risikoene som virksomheten står overfor.

I kapittel 6 stiller KD krav om ledelsessystem for informasjonssikkerhet. Det anbefales at dette utformes etter kjente standarder som ISO/IEC 27001. I standarden ISO 27001:2013 skal også sikkerhetsområder som personellsikkerhet, fysisk sikring, adgangskontroll og tilgangsstyring være dekket med egne rutiner eller retningslinjer. Et allerede etablert ledelsessystem for informasjonssikkerhet og personvern kan være et godt utgangspunkt å utvide og bygge rundt. Eventuelt med overordnede sikkerhetsmål og -strategier, med tilpasning eller tilførsel av nye sikkerhetsroller, og med sammenheng mellom aktuelle retningslinjer og rutiner.

Ved å se sammenhenger mellom ledelsessystemet for informasjonssikkerhet og personvern, styringssystemet for sikkerhet og virksomhetsstyringen for øvrig, kan virksomhetene oppnå en helhetlig tilnærming til sin sikkerhetsstyring og organisere sine ressurser på en hensiktsmessig måte. Viktige roller vil være sikkerhetsleder og eventuelt autorisasjonsansvarlig, se punkt 7.2.

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.

[31] Virksomhetssikkerhetsforskriften § 3.

7.2 Sikkerhetsklarering og autorisasjon

Virksomheter som håndterer informasjon som er sikkerhetsgradert etter sikkerhetsloven må ha ansatte som er sikkerhetsklarert og/eller autorisert for aktuelt nivå i henhold til sikkerhetsloven.

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.[32]

Det er den enkelte virksomhets ansvar å sørge 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 av ansatte skal den enkelte virksomhet fylle ut personopplysningsblankett og oversende denne til SKM *via KD.*

- Autorisasjon gjennomføres i den enkelte virksomhet. En forutsetning for at virksomheten kan autorisere egne ansatte er at styringssystem for sikkerhet er på plass, se punkt 9.1. Det skal gjennomføres en autorisasjonssamtale før det gis autorisasjon. Virksomhetens leder er autorisasjonsansvarlig.[33] Ved behov kan autorisasjonsansvaret delegeres, for eksempel til sikkerhetsleder. KD besørger autorisasjon av virksomhetens leder, eller eventuelt sikkerhetsleder/ansvarlig.

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

7.3 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.

Departementet skal innenfor sitt ansvarsområde identifisere og holde oversikt over GNF og virksomheter som råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for GNF.

Kunnskapsdepartementets virksomhet, handlingsfrihet og beslutningsdyktighet er definert som en GNF. Det omfatter departementets rolle som faglig sekretariat for politisk ledelse, utøvelse av myndighet og styring og oppfølging av underliggende virksomheter.

Arbeidet med å identifisere GNF i KDs sektor er pågående, og over tid vil hva som er GNF også kunne endres i takt med samfunnsutviklingen.

---

[32] Sikkerhetsloven § 8-1.

[33] Sikkerhetsloven § 8-9.

7.4 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 KDs underliggende virksomheter, og 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 enda 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:

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

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.

8 Kritisk infrastruktur og kritiske samfunnsfunksjoner

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*, og omfatter blant annet matforsyning, bank og finans, olje og gass, elektronisk kommunikasjon, satellittbasert kommunikasjon og navigasjon, transport og kraft.

I oversikten i *Samfunnets kritiske funksjoner*[34] den til enhver tid justerte versjonen av denne i JDs årlige budsjettproposisjon[35], er det definert 14 kritiske samfunnsfunksjoner. Åtte departementer er utpekt som hovedansvarlig for ett eller flere av de 14 områdene. KD er ikke blant disse, 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" (jf. 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 koronapandemien.[36]

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

[34] DSB (2016): Samfunnets kritiske funksjoner.

[35] JD (2020): Prop. 1 S (2020–2021), tilgjengelig på: https://www.regjeringen.no/no/dokumenter/prop2.-1-s-20202021/id2768489/

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

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.** Uninett AS utvikler og driver det norske forskningsnettet. Forskningsnettet forbinder mer enn 200 norske utdannings- og forskningsinstitusjoner og over 300 000 brukere, 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 Uninett AS, og brukes både av høyere utdanning, grunnskolen, videregående skole og mange forskningsinstitusjoner. Løsningen har ca. 180 millioner årlige innlogginger.

Departementer som er hovedansvarlige for kritiske samfunnsfunksjoner og tilhørende infrastruktur skal blant annet ha oversikt over risiko og gjennomførte/planlagte beredskapstiltak på området.

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.

9 Kunnskapsoverføring og internasjonalt akademisk samarbeid

Norske universiteter, høgskoler og forskningsinstitutter skaper og forvalter 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 kunnskapssektoren 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 avdekke denne typen forsøk på informasjonsinnhenting.

9.1 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, vil KD ta initiativ til å utvikle nasjonale retningslinjer for ansvarlig internasjonalt samarbeid. Retningslinjene skal bygge opp under institusjonenes eget sikkerhets- og beredskapsarbeid, og være et praktisk verktøy for institusjoner, enkeltforskere og studenter. 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.

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.

Dette kapittelet vil oppdateres med henvisning til retningslinjene når disse er ferdigstilte.

9.2 Ulovlig kunnskapsoverføring – 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 sensitiv kunnskap, og er beskyttet av eksportkontrollregelverket med et tilhørende lisenssystem.

Med sensitiv kunnskapsoverføring menes enhver form for deling av kunnskap om lisenspliktige varer og teknologi, eller annen kunnskap som kan ha militær anvendelse. Utenriksdepartementet er ansvarlig myndighet for gjennomføring av eksportkontrollen i Norge. Utenriksdepartementet har utarbeidet egne retningslinjer for kunnskapssektoren (2020).[37]

I Meld. St. 35 (2020-2021) *Eksport av forsvarsmateriell fra Norge i 2020, eksportkontroll og internasjonalt ikke-spredningssamarbeid* er det en økende erkjennelse av at norske kunnskaps- og teknologimiljøer utsettes for forsøk på omgåelser av eksportkontrollregelverket. 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 Norge 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

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

internasjonalt nivå innen kunnskapsområder som har militær anvendelse eller som kan benyttes i utviklingen av masseødeleggelsesvåpen (MØV). Undervannsteknologi og materialteknologi er eksempler på kunnskap som vi vet utenlandske aktører forsøker å anskaffe fra Norge til militær bruk i hjemlandet. De siste årene er flere forsøk på ulovlig kunnskapsoverføring fra Norge avdekket og hindret.

UD har sett behov for å tydeliggjøre hva som er lisenspliktig kunnskapsoverføring, når lisensplikten inntrer, og hvordan man skal søke om lisens fra UD. De vil legge opp til en ny lisensieringspraksis hvor man må søke om tillatelse før informasjonsdeling finner sted, i tilfeller der man skal overføre kunnskap som kan anvendes til militær bruk til utenlandske borgere. Dette kapittelet vil oppdateres med henvisning til oppdaterte forskriftsendringer og veileder for kunnskapssektoren når disse er vedtatt. Beredskapsrådet har satt ned en arbeidsgruppe for å utarbeide en ny veileder for arbeidet med eksportkontroll i tråd med de varslede forskriftsendringene, og dette kapittelet vil oppdateres med henvisning til også denne når denne er ferdigstilt.[38]

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 styringssystem for informasjonssikkerhet. Vi anbefaler å gjennomgå UDs og Beredskapsrådets veiledere 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 kunnskapsoverføring, samt sørge for ledelsesforankring av dette arbeidet. Det kan være hensiktsmessig å utnevne roller med særskilt ansvar for å søke om eksportlisenser.

10 Særskilte tiltak og ressurser

10.1 Nasjonalt beredskapssystem

Det er utarbeidet et sikkerhetsgradert Sivilt beredskapssystem (SBS), som sammen med Beredskapssystem for Forsvaret (BFF) utgjør Nasjonalt beredskapssystem (NBS). KD har med bakgrunn i SBS utarbeidet KDs beredskapsplan (KDBP). Denne inneholder en rekke tiltak knyttet til sektoroverskridende kriser i fredstid forårsaket av alvorlige tilsiktede hendelser, sikkerhetspolitiske kriser eller væpnet konflikt eller trusler om slike. Planverket inneholder tiltak som gjelder departementet selv og noen øvrige virksomheter i sektoren.

10.2 Veiledningsmateriell

Veiledningsmateriell som gjelder forebygging og beredskapsarbeid for barnehager og utdanningsinstitusjoner er tilgjengelig på Udir sine nettsider. Udir, DSB, Politidirektoratet og Helsedirektoratet

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

har laget en ny veiledning med tittelen *Hvordan håndtere alvorlige hendelser i barnehage og skole* som nylig er publisert på denne siden. Veilederen gir råd om praktisk beredskapsarbeid.

Politidirektoratet 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.

Alle virksomheter har et ansvar for å sikre egen aktivitet mot terrorhandlinger. NSM, PST og Politidirektoratet (POD) har i den forbindelse utgitt en veileder for offentlige og private virksomheter: Terrorsikring: Veileder i sikkerhets- og beredskapstiltak mot tilsiktede uønskede handlinger og Råd mot terrorhandlinger.

Formålet med veilederen er å gi virksomhetene et hjelpemiddel til å utarbeide tidsbegrensede sikkerhetstiltak for å møte en terrortrussel. Behovet for å iverksette slike tiltak kan oppstå ved endringer i 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.

Regjeringen har utarbeidet en nasjonal veileder for forebygging av ekstremisme og voldelig radikalisering 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.

10.3 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 UH-sektoren. De 14 medlemmene av rådet er representanter for statlige og private universiteter og høyskoler, fagskoler, studentsamskipnader og folkehøyskoler.

Rådet har i 2021 14 medlemmer som er valgt på ulike måter og basert på ulike kriterier. Rådet velger selv ett av medlemmene som leder for en periode på normalt to år. Universitetet i Stavanger (UiS) ivaretar sekretariatsfunksjonen for rådet og er kontaktpunkt mot KD.

En viktig oppgave for rådet er å legge til rette for at det kan utvikle seg en samordnet praksis innen høyere utdanning på områder der det vurderes hensiktsmessig, og bidra til deling av beste praksis og erfaring mellom virksomhetene. Rådet skal blant annet bidra til at private virksomheter tilegner seg kunnskap om krav og føringer som er gitt fra myndighetene til de statlige institusjonene. I tillegg har rådet til hensikt å stimulere det lokale samarbeidet innenfor samfunnssikkerhet og beredskap, der kommuner, nødetater, frivillige organisasjoner, relevante næringslivsvirksomheter og andre er inkludert.

Temaer det kan være aktuelt for rådet å ta opp er ROS-analyser, krise- og beredskapsplaner, krise-organisering, kriseøvelser, fysisk sikring og informasjonssikkerhet, samt andre temaer med grense-flater mot samfunnssikkerhet og beredskap, som forebygging av radikalisering og voldelig ekstremisme blant studenter.

I forbindelse med sistnevnte tema ble det vinteren 2019 publisert en «Tiltaksliste mot radikalisering og voldelig ekstremisme» som ble utarbeidet av Beredskapsrådet på oppdrag fra KD. Listen er sendt ut til hele UH-sektoren, og politisk ledelse i KD har uttrykt klar forventning om at relevante tiltak blir fulgt opp og implementert i den enkelte virksomheten. Beredskapsrådet har samarbeidet med sikresiden.no om informasjon om dette temaet, herunder e-læring.

10.4 Sikresiden.no

En forutsetning for forebyggende sikkerhetsarbeid og hensiktsmessig håndtering av kritiske situasjoner, er den enkeltes personlige handlingskompetanse. Hver medarbeider og student skal vite hva vedkommende selv kan gjøre i ulike situasjoner og hvor en kan få hjelp. Opplæring og relevant informasjon er derfor avgjørende, og bidrar både til å redusere risiko og tilfredsstille 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 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 grunnlaget for en mer helhetlig sikkerhetskultur 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 2021 har om lag 400 000 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 løsningen må den brukes aktivt. 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 skoleskytings- eller terrorsituasjon, ved selvmordsfare, forebygging av ekstremisme, brannforebygging, før utenlandsreiser, i personvern- og informasjonssikkerhetsopplæring, samt brukes i sikkerhetsmåneden og i beredskapsøvelser.

OsloMet, UiO og UiB har initiert og drevet fram sikresiden.no, med bidrag fra Uninett AS og andre. Sikresiden.no forvaltes fra OsloMet, og alle som deltar i sikresiden-samarbeidet spleiser på utgiftene til forvaltning, drift og utvikling.

11 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.

- Utdanningsdirektoratet: Sikkerhet og beredskap
- Justis- og beredskapsdepartementet: Generelt om samfunnssikkerhet
- Kunnskapsdepartementet: Generelt om samfunnssikkerhet i kunnskapssektoren
- Direktoratet for samfunnssikkerhet og beredskap (DSB): Risiko, sårbarhet og beredskap
- Direktoratet for samfunnssikkerhet og beredskap (DSB): Kriseinfo
- Sikresiden: Sikresiden.no
- Helsedirektoratet: Forskrift om miljø og helse i barnehagen
- Nasjonal sikkerhetsmyndighet (NSM): Publikasjoner, veiledere, kurs og konferanser
- Statens strålevern: Strålevern og atomsikkerhet
- Nasjonalt utdanningssenter for samfunnssikkerhet og beredskap (NUSB): Kurs og utdanningstilbud innen samfunnssikkerhet og beredskap
- Norsk Senter for Informasjonssikring (NorSIS): Veiledere, seminarer/konferanser om internkontroll og informasjonssikkerhet
- Kommunal informasjonssikkerhet (KINS): Seminarer/konferanser om informasjonssikkerhet
- Datatilsynet: Personvern
- Digitaliseringsdirektoratet (Digdir): Veiledere om informasjonssikkerhet
- Norsk brannvernforening: Informasjon, opplæring og rådgivning om brannvern
- Beredskapsrådet: Rådet for samfunnssikkerhet og beredskap i kunnskapssektoren
- Unit: Direktoratet for IKT og fellestjenester i høyere utdanning og forskning
- Uninett AS: Kunnskaps-Norges IKT-infrastrukturselskap
- Politiets sikkerhetstjeneste (PST): Trusselvurderinger og informasjon
- Etterretningstjenesten: Fokus - Forsvaret