Sikt
Kunnskapssektorens tjenesteleverandør

VERDIOVERSIKT

En veileder for universiteter, høgskoler og forskningsinstitutter

Cybersikkerhetssenter for forskning og utdanning
eduCSC

Versjon	1.0 / 01.2023
Skrevet av	Randi Utstrand

Sikt – Kunnskapssektorens tjenesteleverandør
Telefon: 73 98 40 40 | Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Org.nr: 919 477 822
Besøksadresser: Trondheim: Abels gate 5 – Teknobyen ● Oslo: Fridtjof Nansens vei 19 ● Bergen: Harald Hårfagres gate 29
Postadresse: Abels Gate 5A, 7030 Trondheim

Innholdsfortegnelse

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

Innledning

Sikkerhetsarbeidet er til for å sikre virksomhetens samfunnsoppdrag, kjernevirksomhet og alt som understøtter dette. Dette er mange lag med *verdier*. Verdiene er nødvendige for virksomhetens leveranse- og utviklingsevne, og ivaretar mer overordnede konsekvenskategorier som økonomi, omdømme og kvalitet.

Verdier er funksjoner, prosesser, tjenester og kvaliteter, som for eksempel evnen til å produsere ny kunnskap, eller tillit til informasjon. Verdier er også informasjon, datanettverk, laboratorieutstyr og bygninger. Alle disse verdiene har ulik betydning for virksomhetens evne til å oppfylle sitt samfunnsoppdrag og til å nå sine mål.

Verdier kan også ha betydning for landets samfunnssikkerhet og beredskap. I spesielle tilfeller kan de også ha betydning for nasjonale sikkerhetsinteresser, og for de grunnleggende nasjonale funksjoner. Da omtales de som skjermingsverdige, og skal beskyttes etter sikkerhetslovens bestemmelser.

Virksomhetens oversikt over egne verdier er utgangspunktet for sikkerhetsstyringen med tiltak, og for planlegging av beredskap og kontinuitet. Verdioversikt er derfor viktig, men det kan være krevende å gjøre verdivurderingene som må til for å faktisk bestemme «en verdi». Det er også en utfordring å dele verdiene i ulike lag, og finne formen på det som kan sies å være virksomhetens verdioversikt.

Denne veilederen tar utgangspunkt i at virksomhetene kan få bedre verdioversikt, ved å gjennomføre verdivurderinger som en del av styringsaktivitetene for sikkerhet. Verdioversikten vil bygges over tid, i takt med sikkerhetsstyringen.

Veilederen sammenstille og forklare de mest sentrale føringer og kriterier for verdivurdering, med stor grad av henvisninger videre til Nasjonal sikkerhetsmyndighet (NSM) sine veiledninger og håndbøker.

Formålet med veilederen er å gi hjelp til å finne informasjonsverdier som har beskyttelsesbehov, som kan være utsatt for sikkerhetstruende hendelser, eller som er skjermingsverdige etter sikkerhetsloven.

Innholdet i veilederen er utarbeidet på bakgrunn av mange samtaler og mye erfaringsdeling fra ressurspersoner i forskning og utdanning.

Vi håper veilederen vil være til nytte.

Eventuelle uklarheter i innholdet kan meldes inn til kontakt@sikt.no.

Cybersikkerhetssenter for forskning og utdanning - 2023

Føringer og avgrensning

Styringsdokumentet for arbeid med sikkerhet og beredskap i Kunnskapsdepartementets sektor[1] stadfester krav som fordrer verdioversikt:

1. **Kapittel 7[2] sier at alle virksomhetene underlagt KD er omfattet av sikkerhetsloven.**
- Dette betyr at virksomhetene skal ha et styringssystem for sikkerhet, som er samordnet ledelsessystemet for informasjonssikkerhet og personvern[3] og øvrig virksomhetsstyring.
- Virksomhetene skal ha en tydelig sikkerhetsorganisasjon med definerte roller og ansvarsområder.
- Det er krav om å vurdere, kartlegge og holde oversikt over virksomhetens skjermingsverdige verdier, som *informasjon, informasjonssystemer, infrastruktur eller objekter*[4]

I Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning[5] punkt 2 gis det nærmere krav til oversikt over informasjon og informasjonssystemer.

I dagligtale omtales disse to verdikategoriene gjerne under ett, som *informasjonsverdier*. Dette følger også HK-dir sin terminologi i tilstandsrapporten av 2022, s. 18[6], som benytter samlebetegnelsen *informasjonsverdier* på samme vis. Dette er hensiktsmessig, da informasjon og informasjonssystemer henger så tett sammen, i informasjonsbehandlingen som vi utøver.

Når vi skal ha oversikt over *informasjonsverdier*, snakker vi egentlig om flere vurderingsprosesser:

- Kategorier eller typer av informasjon eller informasjonsbehandling
- Hvordan vi vurderer informasjonen eller informasjonsbehandlingens betydning
- De enkelte informasjonssystem, eller flere system som sammen representerer en verdi
- Hvordan vi vurderer informasjonssystemenes betydning

En *informasjonsverdi* kan derfor sies å være noe vi både har vurdert typen, størrelsen og avgrensningen til, og også vurdert betydningen av.

En virksomhet sin oversikt over informasjonsverdier, er dermed *den oversikten* virksomheten til enhver tid har over sin informasjon og informasjonsbehandling, sine informasjonssystemer, og verdien disse er vurdert til å representere. Vi vil på den bakgrunn si i at verdioversikten kan bygges gjennom å faktisk gjøre verdivurderinger.

En antagelse er dog at verdioversikten aldri kan bli helt fullstendig, eller helt sammenstilt.

Det kan være at informasjon eller informasjonsbehandling ikke alltid passer som en definert type eller i en kategori, eller at et informasjonssystem ikke kan defineres eller sees i sammenheng med andre.

Forhold som avgjør informasjonsverdienes betydning, vil alltid være i endring.

---

[1] Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor - regjeringen.no
[2] Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor - regjeringen.no
[3] F-04-20 Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning - regjeringen.no
[4] Virksomhetssikkerhetsforskriften § 2
[5] rundskriv-f-04-20.pdf (regjeringen.no)
[6] Informasjonssikkerhet og personvern i høyere utdanning og forskning (hkdir.no)

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

Verdioversikten bygges i flere lag

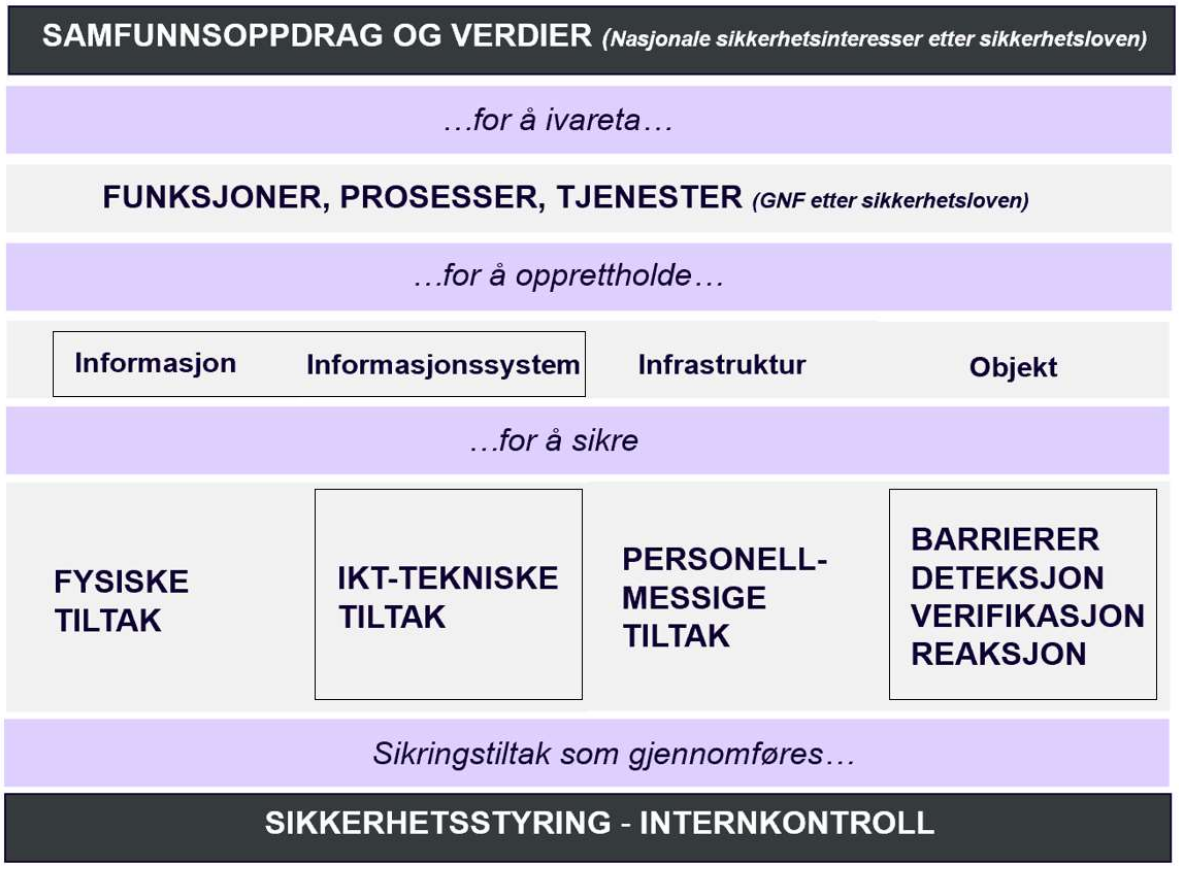
Denne veilederen tar utgangspunkt i at oversikten over informasjonsverdier bygges lagvis, gjennom å gjøre verdivurderinger. Når vi skal gjøre verdivurderinger, må forholdene som avgjør informasjonsverdienes betydning sees i riktig og stor nok kontekst. For å vise hvordan dette henger sammen, er det til nytte å ta utgangpunkt i sikkerhetsstyringens formål.

Sikkerhetsstyringens formål illustreres under med en modell som NSM benytter i sin forklaring av forebyggende sikkerhetsarbeid etter sikkerhetsloven. Vi har bearbeidet modellen slik at den kan gjelde for en virksomhet i forskning og utdanning sitt overordnede bilde på egen verdioversikt som sikkerhetsarbeidet er til for.

(NB: De tynne rammene i modellen er lagt inn for å henvise til hvilke områder eduCSC har sin hoved kompetanse på).

Enkelt oppsummert, så sier denne modellen at *sikkerhetsstyring* er et internkontrollområde som skal sikre *informasjon, informasjonssystemer, infrastruktur* og *objekter fra tilsiktede handlinger,* med sikringstiltak innenfor *ulike tiltaksområder*. Sikringstiltakene skal sørge for at *funksjoner, prosesser* og *tjenester* opprettholdes, slik at virksomhetens *samfunnsoppdrag* og *verdiskaping* ivaretas.

Les modellen nedenfra og opp!



Med modellen over som utgangspunkt foreslår denne veilederen at oversikt over informasjonsverdier bygges lagvis.

Dette er fordi verdiene har et forhold til hverandre, og må sees i kontekst av de ulike lagene når verdienes betydning skal vurderes.

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

1. Forhold av betydning for verdivurderingen

Metoden for verdivurdering vil være avhengig av typen, størrelsen eller omfanget av informasjonsverdien, og hvilke kriterier som blir gjeldende. Dersom vi tillater oss å kalle funksjoner, prosesser og tjenester for en type *sammensatt informasjonsverdi*, vil vi måtte vurdere den på et noe annet grunnlag enn hvordan vi vurderer verdien til et sett med ubehandlede rådata i et forskningsprosjekt. Vi vil se at det er noen bestemte metoder for å gjøre verdivurdering av informasjon, av informasjonssystem, og av et sett med informasjonsbehandlinger som til sammen utgjør en funksjon, prosess eller tjeneste.

1.1 Prinsippene for informasjonssikkerhet

For å finne kriteriene og metodene, starter vi med det helt grunnleggende, som er prinsippene for informasjonssikkerhet; konfidensialitet, integritet og tilgjengelighet (KIT).

Konfidensialitet *handler om at informasjonen ikke skal bli kjent for uvedkommende (K)*

Integritet *handler om at informasjonen ikke blir endret av uvedkommende, eller ved et uhell (I)*

Tilgjengelighet *handler om at informasjonen er tilgjengelig ved behov, eller går tapt (T)*

Verdivurdering av informasjon på bakgrunn av KIT omtales også som klassifisering av informasjon, fordi vi plasserer informasjonen i ulike «klasser». Klassifiseringsnivået vi gir sier noe om hva slags beskyttelses- eller sikringsbehov informasjonen bør ha, og om det er nødvendig med ytterligere risikovurdering av informasjonsbehandlingen, og av informasjonssystemene som inngår.

Verdivurdering og klassifisering av informasjon er derfor helt grunnleggende for informasjonssikkerheten, og for det helhetlige sikkerhetsarbeidet i virksomheten.

I verdivurderingen må vi vurdere informasjonsverdiene i kontekst av hvilke lovkrav som gjelder. Vi må ha et oppdatert trusselbildet som er relevant for informasjonsverdienes formål og behandling, og hvordan disse kan ha betydning for samfunnssikkerheten og for nasjonale sikkerhetsinteresser. Det er også viktig å vurdere informasjonsverdienes betydning for egen virksomhet, og hvordan disse understøtter kjernevirksomheten og overordnet samfunnsoppdrag.

Når vi vurderer K, I og T, må vi derfor tenke i lengre linjer og over flere lag. På den måten får vi med oss alle forholdene som faktisk er relevante og har betydning for hvordan vi skal fastsette informasjonens verdi, og dermed også beskyttelsesbehov.

1.2 Lovkrav

For å få bedre forståelse av kravene som ligger til grunn når verdioversikt skal bygges, tar vi først en kort henvisning til hvilke lover som får en særlig betydning for informasjonsverdiene i forskning og utdanning. Det er gjerne konfidensialitetsprinsippet som er lettest å se at er ivaretatt av lovverket, men vi vil se at også integritet og tilgjengelighet har stor betydning.

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

Offentlighetsloven[7] må være vårt utgangspunkt, og den sier at offentlig virksomhet som hovedregel skal være åpen og gjennomsiktig. Dette er blant annet for å styrke informasjons- og ytringsfriheten, demokratisk deltakelse, rettssikkerheten vår, og tilliten til det offentlige. Den har likevel bestemmelser som sier at informasjon også kan unntas offentligheten og retten til innsyn.

Universitets- og høyskoleloven [8]sier at universiteter og høyskoler skal sørge for åpenhet om resultater fra forskning eller faglig eller kunstnerisk utviklingsarbeid. Ansatte har rett til å offentliggjøre sine resultater, og skal også sørge for at slik offentliggjøring skjer. Loven sier at det ikke kan avtales eller fastsettes varige begrensninger i retten til å offentliggjøre resultater utover det som følger av andre lovverk.

For at formålet med offentlig og åpen informasjon fra forskning og utdanning skal oppnås for samfunnet, må informasjonen også være til å stole på, og den må være tilgjengelig.

Disse to *generelle lovene* sier altså at hovedregelen er offentlighet og åpenhet. Det er likevel andre lover og særlover som gjør seg gjeldende, som har krav til at informasjon ikke skal være åpen, og som fordrer verdioversikt. Vi går nærmere inn på noen av dem. En mer dekkende oversikt finnes i vedlegg 1 til Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning[9]

1.2.1 Personopplysningsloven

Personopplysninger er en type informasjonsverdi, som beskyttes av strenge regulatoriske krav.

Personopplysningsloven[10] regulerer behandlingen av personopplysninger, og den inneholder noen personvernprinsipper[11] som alle virksomheter må følge. Ett av prinsippene er ansvarlighet. Dette prinsippet går ut på at virksomheten skal ha full oversikt over sin behandling av personopplysninger og iverksette tekniske og organisatoriske tiltak som gjør at loven følges.

Gjennom å holde sin protokoll for behandlingsoversikt [12]oppdatert, har virksomhetene oversikt over denne kategorien informasjonsverdi. Det er viktig at personopplysninger som behandles får riktig klassifiseringsnivå, og at risikovurderinger og personvernkonsekvensvurderinger gjennomføres.

Det er også slik at personopplysningsloven bestemmer at det er noen såkalte særlige kategorier personopplysninger [13](sensitive personopplysninger) som det i utgangspunktet er forbud mot å behandle, og som det er knyttet unntak og forbehold til. Dette er også viktige bestemmelser å være klar over, i arbeidet med verdioversikt.

Personopplysninger er en type informasjonsverdi vi finner vi på tvers av forskning, utdanning, støttetjenester og arbeidsprosesser. Internkontrollen for personopplysninger er en del av det systematiske arbeidet med informasjonssikkerhet, og dermed en del av sikkerhetsstyringen.

---

[7] Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova) - Lovdata
[8] https://lovdata.no/lov/2005-04-01-15/§1-5
[9] rundskriv-f-04-20.pdf (regjeringen.no)
[10] Lov om behandling av personopplysninger (personopplysningsloven) - Lovdata
[11] Personvernprinsippene | Datatilsynet
[12] Føre protokoll | Datatilsynet
[13] Behandlingsgrunnlag | Datatilsynet

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

1.2.2 Eksportkontrolloven

Regelverket for eksportkontroll står i kontrast til åpenhet og internasjonalt samarbeid i forskning og utdanning. Eksportkontrollloven[14] er en *særlov* som sier at:

> *§1.*
> *Kongen kan bestemme at varer og teknologi som kan være av betydning for andre lands utvikling, produksjon eller anvendelse av produkter til militært bruk eller som direkte kan tjene til å utvikle et lands militære evne, samt varer og teknologi som kan benyttes til å utøve terrorhandlinger, jf straffeloven § 131, ikke må utføres fra Norge uten særskilt tillatelse. Det kan også settes forbud mot at det uten særskilt tillatelse ytes tjenester som nevnt i første punktum. Det kan settes vilkår for tillatelsene.*

Forskrift om eksport av forsvarsmateriell, flerbruksvarer, teknologi og tjenester[15]går nærmere inn på hva dette regelverket innebærer, og viser til spesifikke varelister [16]og øvrige områder [17]som er regulert av disse bestemmelsene. Dette kalles som *flerbruksteknologi*. Forskriften gjelder også for *immateriell teknologi*, som forstås som *kunnskap om teknologi,* og for det som kalles *sensitive fagområder*. Dette omtales som kontroll av kunnskapsoverføring[18], ved at kunnskapsoverføring i noen tilfeller vil kreve lisens eller forhåndstillatelse av UD.

Eksportkontrollregelverket har betydning for virksomhetene i forskning og utdanning. Utenriksdepartementet (UD) har derfor utarbeidet egen Retningslinje for kontroll med kunnskapsoverføring[19], som må følges. I punkt 1 i retningslinjen står det at utdanningsinstitusjonene må vurdere sensitiviteten i fagområdene og emnene som tilbys ved deres institusjon og vurdere hvorvidt overføring av kunnskap til personer av enkelte nasjonaliteter vil være i strid med norsk eksportkontrollregelverk.

Kontroll av kunnskapsoverføring er for tiden gjenstand for endringsforslag til den gjeldende forskriften[20]. Uavhengig av eventuelle endringer i forskriften, vil det være en myndighetspålagt kontroll av kunnskapsoverføring som er relatert til varelistene.

> *Virksomhetene må derfor bruke varelistene til dette regelverket og få oversikt over hvilken listeført teknologi og hvilke sensitive fagområder de har. Dette må være en del av verdioversikten, over informasjon, og også til informasjonssystemer, objekter og infrastruktur.*

Kontroll med kunnskapsoverføring bør være en del av det helhetlige sikkerhetsarbeidet[21]. Det har også relevante grensesnitt til ivaretakelse av forskningsetiske prinsipper[22], og til ansvarlig internasjonalt samarbeid[23]. Beredskapsrådet for kunnskapssektoren [24]har samlet ressurser til hjelp i arbeidet med kontroll av kunnskapsoverføring.

---

[14] Lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v. [eksportkontrolloven] - Lovdata
[15] Forskrift om eksport av forsvarsmateriell, flerbruksvarer, teknologi og tjenester - Lovdata
[16] https://lovdata.no/forskrift/2013-06-19-718/§4
[17] https://lovdata.no/forskrift/2013-06-19-718/§7
[18] Kontroll av kunnskapsoverføring - regjeringen.no
[19] Retningslinjer for kontroll med kunnskapsoverføring - regjeringen.no
[20] Høring - forslag til endringer i eksportkontrollforskriften - regjeringen.no
[21] Hva er sikkerhetsstyring? - Nasjonal sikkerhetsmyndighet (nsm.no)
[22] Tema | Forskningsetikk
[23] https://hkdir.no/vaare-tenester/retningslinjer-for-ansvarlig-internasjonalt-samarbeid
[24] Eksportkontroll i kunnskapssektoren | Universitetet i Stavanger (uis.no)

1.2.3 Sikkerhetsloven

Sikkerhetsloven[25] med tilhørende forskrifter trådte i kraft 1. januar 2019. Loven skal bidra til å forebygge, avdekke og motvirke *tilsiktede handlinger* som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser og grunnleggende nasjonale funksjoner. [26]

§ 1-1.Formål

Loven skal bidra til

a. *å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser.*
b. *Å forebygge, avdekke og motvirke sikkerhetstruende virksomhet*
c. *At sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.*

Sikkerhetsloven gjelder for statlige, fylkeskommunale og kommunale organer og for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser.

Sikkerhetsloven gjelder også for statlige universiteter, høgskoler og forskningsinstitutter, og kravet om å beskytte skjermingsverdig informasjon[27] må følges. Informasjon er skjermingsverdig [28]dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig. Det er derfor helt nødvendig å ha oversikt over eventuelle skjermingsverdige verdier.

Skjermingsverdig informasjon skal *graderes,* og skjermingsverdige informasjonssystemer skal *klassifiseres* etter klare bestemmelser i sikkerhetsloven. Dette kommer vi nærmere tilbake til.

Vi anbefaler å lese sikkerhetsloven for å bli kjent med bestemmelsene.

1.2.4 Virksomhetssikkerhetsforskriften

I virksomhetssikkerhetsforskriften[29] utdypes kravene til *hvordan* sikkerhetsloven skal etterleves, i et systematisk og organisert sikkerhetsarbeid.

§2. Definisjoner

I denne forskriften menes med

a. *Skjermingsverdige verdier: skjermingsverdig informasjon, skjermingsverdige informasjonssystemer, skjermingsverdig infrastruktur og skjermingsverdige objekter*

b. *Dokument: en logisk avgrenset mengde med informasjon som er lagret på et medium for senere lesing, lytting, framføring, overføring eller lignende*

c. *Lagringsmedium: en elektronisk eller fysisk enhet for lagring av informasjon til bruk for senere lesing, lytting, framføring, overføring eller lignende.*

---

25 Lov om nasjonal sikkerhet (sikkerhetsloven) - Lovdata
26 Om denne veilederen - Nasjonal sikkerhetsmyndighet (nsm.no)
27 https://lovdata.no/lov/2018-06-01-24/§5-2
28 https://lovdata.no/lov/2018-06-01-24/§5-1
29 Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften) - Lovdata

Oversikt over verdier, og hvilke som er skjermingsverdige er helt sentralt i oppbyggingen av dette kontinuerlige arbeidet.

I kapittel 4 i virksomhetssikkerhetsforskriften[30] beskrives det hvordan virksomhetene skal håndtere og beskytte skjermingsverdig informasjon og informasjonssystemer, ut fra den gradering og klassifisering som er satt.

Vi anbefaler å lese virksomhetssikkerhetsforskriften for å bli kjent med bestemmelsene.

Sikkerhetsloven og virksomhetssikkerhetsforskriften gjelder uansett om virksomheten ikke har skjermingsverdige verdier, og verdioversikten er like fullt grunnleggende for sikkerhetsarbeidet[31]. NSM har veiledere og håndbøker [32]som støtter dette arbeidet, og som gir godt grunnlag for metode og systematikk.

1.2.5 Beskyttelsesinstruksen

Beskyttelsesinstruksen[33] gir krav og føringer til hvordan vi skal angi et beskyttelsesnivå, når informasjon ikke skal være åpen og offentlig av andre grunner enn sikkerhetsloven:

§ 1. Anvendelse

Denne instruks kommer til anvendelse ved behandling av dokumenter som trenger beskyttelse av andre grunner enn de som er nevnt i lov 1. juni 2018 nr 24 om nasjonal sikkerhet (sikkerhetsloven) med forskrifter, jf §4.

Instruksen omfatter dokumenter uavhengig av mediet de er tilgjengelig på.

Beskyttelsesinstruksen angir to beskyttelsesgrader som skal brukes for å beskytte informasjon. Disse beskyttelsesgradene medfører også krav til beskyttelse av informasjonssystemet som informasjonen lever i. Dette kommer vi også nærmere tilbake til.

Vi anbefaler å lese beskyttelsesinstruksen for å bli kjent med bestemmelsene.

Vi har nå gitt en kort introduksjon av lovverk som fordrer verdioversikt, og som er med å angi kriterier, klasser og grader for verdivurdering av informasjon og informasjonssystemer. Disse vi skal komme tilbake til.

Denne oversikten er på ingen måte fullstendig, da det er flere lovverk som er viktige å være kjent med, i arbeidet med å ha oversikt over informasjon og informasjonssystemer. Verdt å nevne som eksempler, er

- Helseforskningsloven
- Helseregisterloven
- Arkivloven
- Forvaltningsloven
- eForvaltningsforskriften

---

[30] https://lovdata.no/forskrift/2018-12-20-2053/§22
[31] Informasjonssikkerhet for skjermingsverdige verdier etter sikkerhetsloven | Digdir
[32] Veiledere og håndbøker til sikkerhetsloven - Nasjonal sikkerhetsmyndighet (nsm.no)
[33] Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen) - Lovdata

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

1.3 Trusselbildet

Med trusselbildet mener vi i utgangspunktet det som truer våre verdier med *intenderte* handlinger.

Vi vet at enkelte norske forsknings- og kunnskapsmiljøer er særlig utsatt for spionasje, etterretning og påvirkning, både i den fysiske verden og gjennom cyberoperasjoner.[34]

Spionasje[35] brukes for å få urettmessig fysisk og digital tilgang til informasjon og kunnskap, og også til flerbruksteknologi og sensitiv kunnskap[36].

Dette betyr noe for oss, når vi skal gjøre verdivurderinger. Vi må vite hvilke andre som er interesserte i våre verdier, og gjerne hvordan trussel aktørene opererer, for å kunne gi riktig beskyttelse.

For å forstå alt som trusselbildet kan romme, må vi også forstå hvilken betydning samfunnsoppdraget vårt har for landets samfunnssikkerhet og beredskap, og for våre nasjonale sikkerhetsinteresser.

Ut fra den forståelsen, kan vi angi nærmere hvilken betydning kjernevirksomheten har for samfunnsoppdraget, og til sist komme ned på informasjon og informasjonssystemenes betydning i dette store bildet.

Hvilken betydning har våre aktiviteter for samfunnssikkerheten og beredskapen i landet vårt?

Hvilken betydning har våre aktiviteter for nasjonale sikkerhetsinteresser?

1.3.1 Betydning for samfunnssikkerhet og beredskap

Samfunnssikkerhetsinstruksen [37]presiserer kravene til departementenes arbeid med samfunnssikkerhet. Formålet er å styrke samfunnets evne til å forebygge kriser og til å håndtere alvorlige hendelser gjennom et helhetlig og koordinert arbeid med samfunnssikkerhet.

Direktoratet for samfunnssikkerhet og beredskap (DSB)[38] har utredet hvilke funksjoner som er såkalt *kritiske* for samfunnssikkerheten. Hensikten er å legge til rette for et målrettet og fokusert samfunnssikkerhetsarbeid.

Kritiske funksjoner handler om hvorvidt funksjonen understøtter Norges

- *Styringsevne og suverenitet*
- *Befolkningens sikkerhet*
- *Samfunnets funksjonalitet*

Forskning og utdanning er ikke nevnt i DSB sin rapport fra 2016, men samfunnssikkerhet omfatter likevel mer enn de utpekte kritiske samfunnsfunksjonene. En rekke offentlige virksomheter kan ha samfunnsoppdrag og funksjoner som er verdt å beskytte med hensyn til samfunnssikkerheten.

Ut fra et overordnet og langsiktig sikkerhetsperspektiv kan vi hente frem følgende samfunnsoppdrag fra forskning og utdanning, som vi kan si er av betydning for samfunnssikkerhet og beredskap:

---

[34] Cyberangrep har blitt hverdagskost - Nasjonal sikkerhetsmyndighet (nsm.no)
[35] Spionasje (pst.no)
[36] Ikke-spredning (pst.no)
[37] Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen) - Lovdata
[38] Samfunnets kritiske funksjoner | Direktoratet for samfunnssikkerhet og beredskap (dsb.no)

- Utdanningssystemet er en forutsetning for demokratiforståelse og aktivt medborgerskap, og dermed understøtter det den demokratiske styreformen vår.
- Utdanningssystemet er også en forutsetning for å bekle kritiske roller i samfunnet vårt, som politi og helsepersonell.
- Utdanningssystemet vårt spiller en rolle for å ivareta samfunnets grunnleggende funksjonalitet og befolkningens sikkerhet.
- Forskning og utvikling er en premissgiver for politiske prosesser og kunnskapsbaserte beslutninger, og nødvendig for at vi skal oppnå økonomisk vekst og utvikling.
- Forskningen kan sies å i visse tilfeller bidra til opprettholdelse av Forsvaret sin operative evne, og har dermed en betydning for vår nasjonale sikkerhet.
- Forskningen deltar i samarbeidsprosjekter med andre samfunnsaktører som understøtter totalforsvaret.
- Forskning og utdanning har sikkerhetsmiljøer som har betydning for totalforsvaret.
- Forskning og utdanning har vist seg å være attraktivt mål for infiltrasjon fra fremmed etterretning.

Samfunnsoppdraget til virksomheter innen forskning og utdanning kan derfor sies å være av betydning, om enn ikke kritisk, for landets samfunnssikkerhet og beredskap.

Det kan likevel være enkeltverdier hos enkelte virksomheter som kan sies ha en kritisk samfunnsfunksjon.

At utdanningssystemet og forskningen er troverdig og har integriteten i behold, er høy betydning for at befolkningen har tillit.

1.3.2 Betydning for nasjonale sikkerhetsinteresser

Nasjonale sikkerhetsinteresser[39] er i sikkerhetsloven §1-5 nr.1[40] definert som

… landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til …

a. de øverste statsorganers virksomhet, sikkerhet og handlefrihet
b. forsvar, sikkerhet og beredskap
c. forholdet til andre stater og internasjonale organisasjoner
d. økonomiske stabilitet og handlefrihet
e. samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet.

NSM[41] utdyper at de nasjonale sikkerhetsinteressene er utgangspunkt for:

- Hvorvidt, og på hvilket nivå, informasjon skal anses som *skjermingsverdig* og/eller *sikkerhetsgradert*
- Hvorvidt funksjoner skal anses som *grunnleggende nasjonale funksjoner (GNF)* ved at de er av betydning for statens evne til å opprettholde de nasjonale sikkerhetsinteressene.

Ut ifra funksjonene identifiserer *departementene* virksomheter som er av avgjørende betydning, og utpeker og klassifiserer *skjermingsverdige* objekter og infrastruktur. Sektorprinsippet står altså sentralt i sikkerhetsloven. Det enkelte departement er ansvarlig for forebyggende sikkerhetsarbeid innenfor sitt

[39] Nasjonale sikkerhetsinteresser - Nasjonal sikkerhetsmyndighet (nsm.no)
[40] https://lovdata.no/lov/2018-06-01-24/§1-5
[41] Nasjonale sikkerhetsinteresser - Nasjonal sikkerhetsmyndighet (nsm.no)

ansvarsområde. Departementenes ansvar er beskrevet i sikkerhetsloven § 2-1[42] . Hva som inngår i begrepet nasjonale sikkerhetsinteresser, er utdypet i NSMs veileder i departementenes identifisering av grunnleggende nasjonale funksjoner.

Når virksomhetene skal ha oversikt over skjermingsverdige verdier etter sikkerhetslovens bestemmelser må denne utarbeides i tett rådføring med Kunnskapsdepartementet (KD). Det vil også trolig være hensiktsmessig å rådføre seg med NSM.

Dette betyr at begrepet «skjermingsverdig» må brukes med omhu når vi omtaler våre verdier og hvordan vi har vurdert dem.

1.3.3 Skjermingsverdig informasjon og informasjonssystemer

Informasjonssikkerhetsprinsippene K, I og T ligger til grunn også for vurdering av hvorvidt informasjon[43] eller informasjonssystemer [44]er skjermingsverdige.

§ 5-1. Skjermingsverdig informasjon

Informasjon er skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.

§ 6-1. Skjermingsverdige informasjonssystemer

Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner.

Under følger en enkel forklaring av skjermingsverdig informasjon ut fra K, I og T, hentet fra NSMs veileder i verdivurdering av informasjon[45]

Konfidensialitet
Dersom det kan få *skadefølger for nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende,* så må informasjonens konfidensialitet beskyttes. Skjermingsverdig informasjon som må beskyttes av hensyn til konfidensialitet skal *sikkerhetsgraderes*. Med uvedkommende menes alle som ikke er sikkerhetsklarert og autorisert for informasjonen, og som ikke har et tjenstlig behov for å være kjent med informasjonen.

Om uvedkommende blir kjent med informasjonen anses det som et konfidensialitetsbrudd.

[42] https://lovdata.no/lov/2018-06-01-24/§2-1
[43] https://lovdata.no/lov/2018-06-01-24/§5-1
[44] https://lovdata.no/lov/2018-06-01-24/§6-1
[45] Om denne veilederen - Nasjonal sikkerhetsmyndighet (nsm.no)

Sikkerhetsgradene som skal benyttes etter Sikkerhetsloven §5-3[46] er:

> *§5 -3. Sikkerhetsgradert informasjon*
>
> *En virksomhet som tilvirker informasjon, skal sikkerhetsgradere og merke informasjonen dersom det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende.*
>
> *Følgende sikkerhetsgrader skal benyttes:*
>
> a. *STRENGT HEMMELIG dersom det kan få helt avgjørende skadefølger*
> b. *HEMMELIG dersom det kan få alvorlige skadefølger*
> c. *KONFIDENSIELL dersom det kan få skadefølger*
> d. *BEGRENSET dersom det i noen grad kan få skadefølger*

Integritet
Dersom det kan få *skadefølger for nasjonale sikkerhetsinteresser at informasjonen blir endret*, så må informasjonens integritet beskyttes. Med integritet menes at informasjonen er korrekt og fullstendig sett i sammenheng med emnet og omfanget som informasjonen har til hensikt å omfatte. Integritetsbeskyttelse innebærer å sørge for at det ikke lar seg gjøre urettmessig å endre innholdet i informasjonen.

Tilgjengelighet
Dersom det kan få *skadefølger for nasjonale sikkerhetsinteresser at informasjonen går tapt eller blir utilgjengelig*, så må informasjonens tilgjengelighet beskyttes. Med tilgjengelighet menes at informasjonen er tilgjengelig for virksomheten innenfor det tidsrommet som virksomheten har behov for å bruke den. Dersom slik informasjon går tapt, eller blir gjort utilgjengelig, anses det som et tilgjengelighetsbrudd. Virksomheten må vurdere tilgjengelighetsbehovene til informasjonen den besitter, og identifisere konsekvenser for nasjonale sikkerhetsinteresser dersom informasjonen ikke er tilgjengelig for de riktige brukerne eller systemene til rett tid.

Ugradert skjermingsverdig informasjon
Begrepet *ugradert skjermingsverdig informasjon* som benyttes i virksomhetssikkerhetsforskriften § 22[47] brukes om informasjon som er skjermingsverdig etter sikkerhetslovens § 5-1, men som *ikke* har et skadepotensiale for nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende.

Ugradert skjermingsverdig informasjon skal beskyttes slik at integritet og tilgjengelighet sikres. Det kan tenkes at ugradert skjermingsverdig informasjon, hvis konfidensialitet ikke må beskyttes etter sikkerhetsloven, likevel har et konfidensialitetsbehov etter annet lovverk og må beskyttes deretter.

NSM har flere gode veiledninger og håndbøker som anbefales for videre lesing:

NSMs Veileder i verdivurdering av informasjon

NSMs Håndbok i verdivurdering av informasjon

NSMs Veileder i håndtering og beskyttelse av sikkerhetsgradert informasjon

NSMs Veileder ugradert skjermingsverdig informasjon og informasjonssystem

Vi anbefaler å lese gjennom disse, for å bli kjent med hva som kan gjelde for egen dere.

[46] https://lovdata.no/lov/2018-06-01-24/§5-3
[47] https://lovdata.no/forskrift/2018-12-20-2053/§22

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

1.4 Informasjonsverdienes betydning for egen virksomhet

Vi har så langt sett på lovverk som har betydning for verdivurderingen, og på trusselbildet i kontekst av samfunnssikkerhet og nasjonale sikkerhetsinteresser.

Det siste forholdet vi omtaler, er virksomhetens egne mål for sikkerhetsarbeidet. Det er viktig å vurdere informasjonsverdienes betydning for egen virksomhet, og hvordan disse understøtter kjernevirksomheten og overordnet samfunnsoppdrag. Det å være i samsvar og overenskomst med lovverk er å anse som minstekrav.

Ved at virksomhetens ledelse selv har vurdert sikkerhet som strategisk viktig for å nå sine overordnede mål, sin evne til å levere på samfunnsoppdraget, til verdiskapning og betydningen for eget omdømme, gjør også noe med hvordan virksomheten vil vurdere betydningen av «sikkerhet i alle ledd».

2. Klassifisering av informasjon

Vi har gått gjennom hvordan skjermingsverdig informasjon skal graderes etter sikkerhetsloven. Disse graderingsnivåene brukes ikke for informasjon som skal beskyttes etter andre krav enn sikkerhetsloven.

Vi har også tidligere omtalt beskyttelsesinstruksen. Denne angir to beskyttelsesgrader [48] som skal anvendes når informasjon *ikke skal være åpen og offentlig av andre grunner* enn sikkerhetsloven.

Beskyttelsesgradene som følger av beskyttelsesinstruksen for å beskytte informasjon er, STRENGT FORTROLIG og FORTROLIG.

Dette er beskyttelsesgrader som i dag brukes av virksomhetene i forskning og utdanning, i den etablerte metodikken og praksis for å klassifisere informasjon. Denne metodikken baserer seg på den tidligere Uninett fagspesifikasjon (UFS) 136, som primært har omhandlet konfidensialitet. Denne er i skrivende stund under revisjon, og vil komme som sektorstandard for klassifisering av informasjon, med 4 nivå for K, I og T:

Konfidensialitet	Integritet	Tilgjengelighet
Åpen	***Lav***	***Lav***
Beskyttet/Intern	***Middels***	***Middels***
Fortrolig	***Høy***	***Høy***
Strengt Fortrolig	***Svært høy***	***Svært høy***

Vi tar en kort gjennomgang av betingelsene for å bruke disse beskyttelsesgradene STRENGT FORTROLIG og FORTROLIG, og de kravene som virksomhetene så er forpliktet til å oppfølge.

[48] https://lovdata.no/forskrift/1972-03-17-3352/§2

Beskyttelsesgradene skal brukes slik, jfr beskyttelsesinstruksen[49]:

> *§ 4. Om bruken av beskyttelsesgrader*
>
> *Når betingelsene for gradering etter § 3 er til stede, benyttes beskyttelsesgradene slik:*
>
> *«Strengt fortrolig» benyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende.*
>
> *«Fortrolig benyttes dersom det vil kunne skade offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende.*
>
> *Det må påses at det ikke benyttes høyere sikkerhetsgrad enn strengt nødvendig.*

Betingelsene i § 3 [50]sier at gradering av et dokument bare skal foretas når dokumentet kan unntas fra offentlighet i samsvar med offentleglova, og skadevirkninger som nevnt i § 4 kan inntreffe.

Disse beskyttelsesgradene medfører krav til beskyttelse både av informasjonen og av informasjonssystemet som informasjonen lever i. Disse kravene er gitt av flere av paragrafene i beskyttelsesinstruksen, og er også tydeliggjort i § 12[51] som sier at:

> *§ 12*
>
> *Dokumenter gradert etter denne instruksen skal så langt det passer, behandles elektronisk i samsvar med følgende regler i sikkerhetslovens forskrift om virksomheters arbeid med forebyggende sikkerhet § 23 i kapittel 4 om håndtering og beskyttelse av skjermingsverdig informasjon, kapittel 7 om beskyttelse av skjermingsverdige informasjonssystemer og sikkerhetslovens forskrift om kryptosikkerhet.*
>
> *Dokumenter gradert etter instruksen skal i slike tilfeller følge reglene for dokumenter gradert BEGRENSET.*

Her må vi merke oss at det står «så langt det passer». Videre må vi ha et forhold til hva det vil si å følge kravene til dokumenter gradert BEGRENSET. Det er tydeliggjort i virksomhetssikkerhetsforskriften kapittel 4 § 22[52]:

> *§ 22*
>
> *Når en virksomhet håndterer en risiko knyttet til ugradert skjermingsverdig informasjon etter § 13, skal tiltakene som et minimum sørge for at informasjonen ikke kan gå tapt, endre eller gjøres utilgjengelig med enkle midler. Dersom risikoen tilsier det, skal informasjonen også beskyttes mot avanserte angrepsmetoder.*
>
> *Når virksomheten håndterer en risiko knyttet til informasjon gradert BEGRENSET, er kravet til et forsvarlig sikkerhetsnivå oppfylt dersom informasjonen ikke med enkle midler kan bli kjent for uautoriserte personer.*
>
> *Ved valg av sikkerhetstiltak skal virksomheten se behovet for å beskytte informasjonens konfidensialitet, integritet og tilgjengelighet i sammenheng og veie hensynene mot hverandre.*

[49] https://lovdata.no/forskrift/1972-03-17-3352/§4
[50] https://lovdata.no/forskrift/1972-03-17-3352/§3
[51] https://lovdata.no/forskrift/1972-03-17-3352/§12
[52] https://lovdata.no/forskrift/2018-12-20-2053/§22

Ut fra disse bestemmelsene kan vi si at dersom vi setter beskyttelsesgraden FORTROLIG eller STRENGT FORTROLIG på informasjonen vår, bør vi gjennomføre risikovurderinger av informasjonsbehandlingen og informasjonssystemene som informasjonen lever i.

Vi understreker at ved å gjennomføre risikovurderinger, bygges også verdioversikt.

2.1 Oversikt over nivåene som utgjør verdivurderingen av informasjon

For å tydeliggjøre et skille mellom skjermingsverdig og ikke skjermingsverdig informasjon, kan vi lage følgende illustrasjon:

IKKE SKJERMINGSVERDIG ETTER SIKKERHETSLOVENS BESTEMMELSER Informasjonen har beskyttelsesbehov av andre forhold		
Konfidensialitet	**Integritet**	**Tilgjengelighet**
Åpen	***Lav***	***Lav***
Beskyttet/Intern	***Middels***	***Middels***
Fortrolig	***Høy***	***Høy***
Strengt Fortrolig	***Svært høy***	***Svært høy***
SKJERMINGSVERDIG ETTER SIKKERHETSLOVENS BESTEMMELSER Informasjonen kan også samtidig ha beskyttelsesbehov av andre forhold		
Konfidensialitet	**Integritet**	**Tilgjengelighet**
BEGRENSET (lavgradert)		
KONFIDENSIELL		
HEMMELIG		
STRENGT HEMMELIG		

Vi har nå gått gjennom et ganske bredt bakteppe for en del forhold som verdivurderinger handler om. Dette mener vi er nødvendig forkunnskap for alle som skal fasilitere og bidra til at virksomhetene får oversikt over sine informasjonsverdier.

Det er fordi vi mener at verdioversikten bygges gjennom å gjøre verdivurderinger.

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

3. Hvordan bygge verdioversikt

En stor del av oversikten over informasjon og informasjonssystemer befinner seg allerede i blant annet IT-porteføljen, i virksomhetens sak- og arkivsystem med journalføring, i de studieadministrative systemer, i lønns- og personalsystemet, i systemene for regnskap og økonomi, i de dokumenterte verdi- og risikovurderinger, i protokoll over behandling av personopplysninger, i oversikt over helsedata og forskningsprosjekter som er meldt inn til de Regionale komiteer for medisinsk og helsefaglig forskningsetikk (REK), og så videre. Listen vil være veldig lang.

Når vi snakker om verdioversikt med formål å beskytte informasjonsverdier fra *intenderte handlinger*, bør vi likevel gjøre verdivurderinger for å finne de verdiene som faktisk kan være utsatt for sikkerhetstruende aktivitet. Vi må også gjøre verdivurderinger for å finne de verdiene som er viktige for virksomhetens evne til å utføre sitt samfunnsoppdrag, og nå sine mål. Dette er en del av sikkerhetsstyringen.

Verdioversikten kan bygges lagvis, gjennom å gjøre verdivurderinger på ulike nivå. Dersom vi ser på modellen som illustrerer sikkerhetsstyringen igjen, får vi et bedre inntrykk av hva disse lagene er:

Vi tror ikke det kan gjøres en grundig nok verdivurdering av informasjon, dersom det ikke tas hensyn til koblingen til kjernevirksomheten, samfunnsoppdraget, og til de nasjonale sikkerhetsinteresser og samfunnssikkerheten.

Derfor anbefaler vi at virksomhetene også gjennomfører verdivurdering av samfunnsoppdraget og kjernevirksomheten sin, og av de *funksjoner, prosesser og tjenester* som understøtter kjernevirksomheten, for å best kunne vurdere verdien av *informasjon* og *informasjonssystemene* sine.

3.1 Verdioversikten må være levende

Vi tror at verdioversikten har mest nytte om den lever i organisasjonen, i alle enheter og lokale miljø. Med det mener vi at det er de ansatte og ledelsen som må ha verdioversikten *i seg og med seg*, i alt de gjør. Dette skaper god sikkerhetskultur. Hva som inngår i de lokale verdioversikter vil være ulikt, fordi kjernevirksomheten med støttefunksjoner favner svært bredt. Samtidig bør det være en viss dokumentert oversikt. Hvordan verdioversikten kan dokumenteres, er det sikkert mange alternativer til, og det overlater vi til virksomhetene å finne ut av.

Vi understreker at en dokumentert oversikt over hva som er virksomhetens mest beskyttelsesverdige verdier som et minimum bør klassifiseres som FORTROLIG eller STRENGT FORTROLIG.

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

I det videre kommer vi med forslag til en struktur for hvordan en levende verdioversikt kan skapes. Vi vil poengtere at det ikke nødvendigvis er slik at man må starte med samfunnsoppdraget og gå stegvis «nedover». Verdivurderinger gjennomføres i virksomhetene allerede, både av informasjon, informasjonssystemer og ulike aktiviteter i kjernevirksomheten. forskningsaktiviteter, som del av risikovurderinger, og ved prioriteringer og valg av sikringstiltak.

Virksomhetene bør tilpasse våre anbefalinger, slik at arbeidet med verdioversikten kan bygge ut og videreutvikle den praksis som virksomheten allerede har.

3.2 Samfunnsoppdraget

Formål	Etablere sikkerhetsmål og prinsipper for sikkerhetsarbeidet, som skal angis i virksomhetens styringsdokument for sikkerhet (Politikk for sikkerhet). *NB: Her bør det bli tydelig at enkelte deler av kjernevirksomheten med støttefunksjoner vil ha behov for sikringstiltak som går ut over det som kan omtales som en slags grunnsikring.*
Hvem	Deltakerne bør være fra øverste ledelse, eller av en gruppe satt sammen av ledelse og medarbeidere i fellesskap.
Hvordan	Dette kan gjennomføres i et møte eller en workshop, som planlegges, forberedes og fasiliteres av sikkerhetsrådgiver med flere. Aktiviteten må forankres hos øverste ledelse. **I workshopen kan man se til** - nasjonale føringer for forskning, utdanning, formidling og nyskaping - tildelingsbrev fra Kunnskapsdepartementet, og andre styringsdokumenter - egne virksomhetsmål, virksomhetsstrategier, satsingsområder og andre interne styringsdokumenter og gjøre vurderinger som sier noe om hvordan sikkerhet er viktig for måloppnåelse.
Dokumenteres	Det som kommer frem i denne runden kan dokumenteres i styrende dokumenter for sikkerhetsstyringen. Det bør også skrives et kort referat eller sammendrag av workshopen, som arkiveres.
Ansvarlig for oppfølging	Sikkerhetsansvarlig er ansvarlig for oppfølging, og sikkerhetsleder eller informasjonssikkerhetsleder, vil trolig være den som gjennomfører oppfølging på vegne av sikkerhetsansvarlig. Roller og ansvar for sikkerhetsarbeidet skal være beskrevet i virksomhetens styringssystem for sikkerhet.

3.3 Kjernevirksomheten

Formål	Finne de områdene av kjernevirksomheten som kan sies å ha beskyttelsesbehov utover det vi kan kalle *grunnsikringen*. Med kjernevirksomhet mener vi i hovedsak forskning, utdanning, formidling og nyskaping. Vi mener ikke fellestjenestene som understøtter kjernevirksomheten. I en slik kartlegging bør «verdistørrelsen» være prosjekt, faggruppe, studieemne, studieprogram eller yrkesutdanning, laboratorier, tungregneanlegg, og lignende. Hensikten er å identifisere hvor det bør gjøres ytterligere verdivurderinger og risikovurderinger, for å finne riktig beskyttelsesnivå. *NB: Merk at slike vurderinger er avhengige av forhold og faktorer som forandrer seg over tid, og må derfor ikke ansees som endelige.*
Hvem	Deltakerne bør være fra øverste ledelse, og inngå i grupper satt sammen av mellomledere og medarbeidere i fellesskap. Vi anbefaler at workshop gjennomføres på tvers av fakulteter, institutter, administrative støttetjenester og teknisk personell. Gjennomfør flere workshoper med ulike grupper. Med tverrfaglig deltakelse vil kreativiteten blir større, og verdivurderingen rikere.
Hvordan	Dette kan gjennomføres i et møte eller en workshop, som planlegges, forberedes og fasiliteres av sikkerhetsrådgiver med flere. **I workshopen kan deltakerne eksempelvis utforske følgende:** *(listen under er kun eksempler, og vil ikke bidra til en dekkende oversikt av kjernevirksomheten til alle virksomhetene i forskning og utdanning)* **Hvilke forskningsområder eller ressurser har vi som:** **Understøtter landets fungering, beslutnings, - og utviklingsevne?** - Her går det å eksempelvis se til FNs bærekraftsmål og til den gjeldende Langtidsplanen for forskning og høyere utdanning. - Eksempler kan være biovitenskap, hav- og klimaforskning, og geologi **Opprettholder, forsterker og forbedrer funksjoner og kvaliteter i samfunnet som har betydning for samfunnssikkerheten, eller for nasjonale sikkerhetsinteresser?** - Dette kan være forskning innenfor geopolitikk og nordområdene våre, statsvitenskap, og andre samfunnsvitenskapelige områder - Det kan være forskning og teknologiområder som er særlig utsatt for spionasje og etterretning fra andre land, som er listet opp i de nasjonale trusselvurderingene, som navigasjons- og sensorteknologi, romfart og satellitteknologi, undervannsteknologi, materialteknologi, datateknologi, IT-sikkerhet og kryptografi, robotikk

	- Det kan være forskning og beregningsmodeller innen helse og velferd som ivaretar samfunnskritiske tjenester. - Det kan være fagmiljø som forvalter forskning, ekspertise og «sannhetsgehalten» i temaer som kan være under press av påvirkningsoperasjoner, for å endre virkelighetsforståelse og beslutningsgrunnlag av nasjonal og global betydning. - Det kan være enkeltpersoner som har spesialistkompetanse som kan gjøre seg gjeldende i situasjoner som berører samfunnssikkerheten, som eksempelvis pandemi. **Er regulert av eksportkontrollregelverket og sanksjonsforskrifter?** - Her må virksomhetene se til varelistene som følger regelverket for å kartlegge laboratorieutstyr og teknologi, kunnskap og informasjon som er omfattet av regelverket. **Hvilke utdanningstilbud har vi som:** **Understøtter de utpekte forskningsområdene**? - Her går det å eksempelvis se til FNs bærekraftsmål og til den gjeldende Langtidsplanen for forskning og høyere utdanning. **Understøtter å bekle kritiske funksjoner i samfunnet?** - Dette kan være innenfor helse, politi og forsvar, og andre mer operative funksjoner av høy betydning. **Hvilke interne sikkerhetsressurser har vi som:** - Forebygger, oppdager og håndterer sikkerhetshendelser, slik at virksomheten har god evne til sikkerhet og beredskap? - Forebygger, oppdager og håndterer sikkerhetshendelser, slik at virksomheten bidrar til god nasjonal evne til sikkerhet og beredskap?
Dokumenteres	Det som kommer frem i workshop kan dokumenteres i eventuelle lokale styrende dokumenter for sikkerhetsstyringen, som gjelder for de enhetene i virksomheten som finner at de har verdier som *kan sies å ha beskyttelsesbehov utover det vi kan kalle grunnsikringen.* Det bør også skrives et kort referat eller sammendrag av workshopen, som arkiveres. NB: Dersom virksomheten vurderer de kan ha skjermingsverdig verdier etter sikkerhetsloven, skal Kunnskapsdepartementet orienteres.
Ansvarlig for oppfølging	Leder av enhet med verdier *som vurderes å ha beskyttelsesbehov utover det vi kan kalle grunnsikringen,* er ansvarlig for at det gjennomføres påfølgende risikovurderinger og sikringstiltak. Sikkerhetsleder og / eller sikkerhetsrådgiver vil bidra i gjennomføringen av oppfølgingen. Roller og ansvar for sikkerhetsarbeidet skal være beskrevet i virksomhetens styringssystem for sikkerhet.

3.4 Funksjoner, prosesser og tjenester

Formål	Finne de *funksjoner, prosesser* og *tjenester* som kan sies å ha beskyttelsesbehov utover det vi kan kalle *grunnsikringen*. *Funksjoner, prosesser* og *tjenester* må forstås som alle de administrative og tekniske fellestjenestene (kan være både lokale og sentrale) som understøtter kjernevirksomheten. Verdivurderingen må handle om fellestjenesten i sin helhet, uavhengig av dens størrelse, eller litt uklare avgrensning. Hensikten er å finne hvilke *funksjoner, prosesser og tjenester* som er av en slik betydning, at *bortfall, eksponering eller feil* påvirker virksomhetens aktiviteter, daglige drift eller troverdighet på en måte som vil ha *alvorlige, eller svært alvorlige konsekvenser.*
Hvem	Dette kan gjøres i grupper satt sammen av ledelse og medarbeidere i fellesskap. Vi anbefaler at workshop gjennomføres på tvers av fakulteter, institutter, administrative støttetjenester og teknisk personell. For dette området må det gjennomfør flere workshoper med ulike grupper for å komme gjennom alle de administrative og tekniske fellestjenestene. Med tverrfaglig deltakelse vil kreativiteten blir større, og verdivurderingen rikere.
Hvordan	Når det kommer til *funksjoner, prosesser og tjenester* som understøtter forskning og utdanning, så har vi ingen standard måte å systematisere og kategorisere disse på. Direktoratet for høyere utdanning og kompetanse (HK-dir, 2022)[53] presenterer en oversikt over 10 hovedkategorier som også vil romme de fleste fellestjenester. Vi anbefaler å ta utgangspunkt i disse kategoriene. Velg inntil 3 kategorier per workshop for å identifisere fellestjenester Vurder så vurdere betydningen av disse.
1. Kategorier for å identifisere fellestjenester: *Identifiser hvilke funksjoner, prosesser eller tjenester i kategorien som finnes i egen virksomhet.*	
Studentadministrasjon *Informasjon som typisk behandles i studentadministrative systemer. Det kan blant annet være navn, fødselsnummer, bosteds- og epostadresse, tidligere utdanning, kurs og emner, semesteravgift, studieprogresjon/-poeng, tilrettelagt undervisning, praksis og eksamensresultater. Det vil også dreie seg om informasjon som behandles i elektroniske kommunikasjonsplattformer som universitetet eller høgskolen tilbyr studentene*	
Læring, vurdering og undervisning *Informasjon knyttet til gjennomføring og administrasjon av undervisning og eksamen eller andre vurderingsformer. Det kan for eksempel være undervisningsplaner, emneinformasjon, pensumlister, eksamensoppgaver og -besvarelser, innleveringer, master- og bacheloroppgaver,*	

[53] Informasjonssikkerhet og personvern i høyere utdanning og forskning (hkdir.no)

bibliotekressurser, nettbaserte læringsressurser og informasjon som behandles om studenter og undervisere i læringsplattformer

Forskning og utvikling

Informasjon om innholdet i, administrasjon og gjennomføringen av forskningsprosjekter. Eksempler på slik informasjon er prosjektbeskrivelser, finansiering, kontrakter, deltakere og samarbeidspartnere, datakilder, rådata, bearbeidede data, forskningsresultater, publikasjoner og kommersielle rettigheter (patenter)

Medarbeidere og ledere

Informasjon om ansettelsesforhold som blant annet behandles i HR-systemer. Det kan være navn, fødselsnummer, bostedsadresse, stilling, lønn, kontonummer, sykefravær, ferie, avspasering, opplæring/kurs, særskilt tilrettelegging, osv. Det vil også omfatte informasjon om personer som ikke er ansatt ved universitetet eller høgskolen, men som mottar godtgjøring for oppdrag, for eksempel sensorer.

Økonomi og regnskap

Informasjon om finansiering av virksomheten og forvaltning og styring av økonomiske verdier. Slik informasjon kan blant annet omhandle budsjetter på virksomhets- og enhetsnivå, årsregnskap, lønnskostnader, prosjektkostnader, bestillinger, utbetalinger og økonomirapporter.

Virksomhetsstyring og strategi

Informasjon om viktige forhold i virksomheten og planer for den videre administrative eller faglige utviklingen, for eksempel utviklingsavtaler med departementet. Informasjon som har betydning for styringen av virksomheten, vil ofte samles i ulike datavarehusløsninger. Dette kan omfatte økonomiske nøkkeldata, studenttall, studiepoengproduksjon, omfanget av eksternfinansiert forskning, ph.d.-programmer, midlertidighet, likestilling og kjønnsbalanse, osv.

Eiendom og fysisk infrastruktur

Informasjon om bygningsmessige forhold og andre deler av det fysiske miljøet. Det kan omfatte informasjon om campus-bygg, byggeprosjekter, laboratorier og -utstyr, heisanlegg, andre elektriske anlegg, osv. Det kan også omfatte ulike typer sensordata om det fysiske miljøet, for eksempel fra adgangskontrollen, varslingsanlegg (brann, vann, fukt), ventilasjon, oppvarming og kameraovervåking.

Informasjon om IT-ressurser og digital infrastruktur

Informasjon om forvaltning og styring av IT-porteføljen. Det kan inkludere informasjon om IT-anskaffelser, datamaskiner, programvare, databaser, tjenesteutsetting og databehandlere, nettverkskonfigurasjon, digital sikkerhet, tilgangsstyring og brukerstøtte.

Media og kommunikasjon

Informasjon som benyttes i det interne og eksterne formidlings- og kommunikasjonsarbeidet. Det vil for eksempel omfatte informasjon på hjemmesider, intranett og i sosiale media (Facebook, Instagram, Twitter, osv.). Det vil også inkludere informasjon om konferanser, seminarer, workshops og deltakere på slike arrangementer.

Alumni

Kontaktinformasjon til tidligere studenter og annen relevant informasjon, for eksempel påmeldinger til nyhetsbrev, arrangementer og sammenkomster.

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

2. **Hvilken betydning har fellestjenesten:** *Gjør en vurdering av hvor viktig de identifiserte fellestjenestene er, ut fra kriteriene under.*	
1. **Liten betydning** Dette innebærer at *bortfall, eksponering eller feil* ved denne fellestjenesten påvirker virksomhetens aktiviteter, daglige drift eller troverdighet på en måte som vil ha få eller ingen merkbare konsekvenser.	
2. **Middels betydning** Dette innebærer at *bortfall, eksponering eller feil* ved denne fellestjenesten påvirker virksomhetens aktiviteter, daglige drift eller troverdighet på en måte som vil ha *merkbare konsekvenser*.	
3. Høy betydning Dette innebærer at *bortfall, eksponering eller feil* ved denne fellestjenesten påvirker virksomhetens aktiviteter, daglige drift eller troverdighet på en måte som vil ha *alvorlige konsekvenser.*	
4. Svært høy betydning Dette innebærer at *bortfall, eksponering eller feil* ved denne fellestjenesten påvirker virksomhetens aktiviteter, daglige drift eller troverdighet på en måte som vil ha *svært alvorlige konsekvenser.*	
Dokumenteres	Det som kommer frem i slike workshoper bør dokumenteres lokalt i virksomheten, hos de ansvarlige eiere av de fellestjenestene som er vurdert. Det bør også skrives et kort referat eller sammendrag av workshopene, som arkiveres. NB: Dersom virksomheten vurderer de kan ha skjermingsverdig verdier etter sikkerhetsloven, skal Kunnskapsdepartementet orienteres.
Ansvarlig for oppfølging	Ansvarlig leder for en fellestjeneste som vurderes å ha høy, eller svært høy betydning er ansvarlig for at det gjennomføres risikovurderinger, at risiko håndteres med sikkerhetstiltak. Det bør vurderes om det skal utarbeides en kontinuitetsplan for fellestjenesten. Informasjonen i fellestjenesten bør klassifiseres. Vurder om det er nødvendig å gjøre risikovurdering av behandlingen av informasjonen i fellestjenesten. Det bør gjøres risikovurderinger av informasjonssystemene som benyttes i fellestjenesten. Sikkerhetsleder og / eller sikkerhetsrådgiver vil bidra i gjennomføringen av oppfølgingen. Roller og ansvar for sikkerhetsarbeidet skal være beskrevet i virksomhetens styringssystem for sikkerhet.

3.5 Informasjon og informasjonssystemer

Formål	Få oversikt over informasjon og informasjonssystemer som har beskyttelsesbehov utover det vi kan kalle grunnsikringen. Dette innebærer også å finne eventuell skjermingsverdig informasjon. Ved å klassifisere informasjonen angir vi beskyttelsesbehovet. Ved å gjøre risikovurdering av informasjon med høye beskyttelsesbehov, kan vi finne riktige sikringstiltak. Med informasjon mener vi all informasjon, data og opplysninger som virksomhetene behandler. Med informasjonssystemer mener vi ulike typer digitale ressurser som benyttes i behandlingen av data og opplysninger, som datamaskiner, programvare, nettverksutstyr, laboratoriemaskiner, osv.
Hvem	Dette kan gjennomføres i et møte eller en workshop, som planlegges, forberedes og fasiliteres av sikkerhetsrådgiver med flere. Dette kan også gjøres individuelt.
Hvordan	Informasjon i forskning og utdanning kan klassifiseres etter gjeldende sektorstandard (UFS 136 under revisjon). Informasjonsverdiene må sees i den sammenhengen og konteksten de er en del av, og ikke som en isolert enhet. Dersom det allerede er identifisert at informasjonen eller informasjonssystemet inngår i en fellesfunksjon som er av en viss betydning for kjernevirksomheten eller andre fellesfunksjoner, eller at informasjonen eller informasjonssystemet inngår i deler av kjernevirksomheten som er vurdert å ha sikkerhetsmessig betydning, eller annen betydning for virksomheten, bør dette hensyntas når klassifiseringen settes. Informasjon som inngår i betydningsfulle fellestjenester, vil trolig ha høye krav til integritet og tilgjengelighet. Informasjon som inngår i forskning og utdanning vil også gjennomgående ha høye krav til integritet og tilgjengelighet. Dersom det er identifisert særlige lovkrav til informasjonen, vil lovkravene ha betydning for hvordan informasjonen skal klassifiseres på konfidensialitet. Det kan også være andre, og virksomhetsinterne forhold som gjør at informasjonen har konfidensialitetsbehov. Dersom det vurderes at det kan få *skadefølger for nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende,* så må informasjonens konfidensialitet beskyttes med *sikkerhetsgradering,* og håndteres etter sikkerhetslovens bestemmelser. Virksomheten skal kontakte Kunnskapsdepartementet for videre prosess og vurdering.
Dokumenteres	Dokumenter som skal unntas offentlighet, skal være påført riktig hjemmelsgrunnlag. Dokumenter kan merkes med angitt K-klasse.
Ansvarlig for oppfølging	Dette skal være fordelt i beskrivelsen av sikkerhetsorganisasjonen. Alle ansatte. Ansvarlige leder eller informasjonseier.

IKKE SKJERMINGSVERDIG ETTER SIKKERHETSLOVENS BESTEMMELSER Informasjonen er ikke skjermingsverdig, men har beskyttelseskrav av andre forhold		
Konfidensialitet	**Integritet**	**Tilgjengelighet**
Åpen	***Lav***	***Lav***
Beskyttet/Intern	***Middels***	***Middels***
Fortrolig	***Høy***	***Høy***
Strengt Fortrolig	***Svært høy***	***Svært høy***
SKJERMINGSVERDIG ETTER SIKKERHETSLOVENS BESTEMMELSER Informasjonen kan også samtidig ha beskyttelseskrav av andre forhold		
Konfidensialitet	**Integritet**	**Tilgjengelighet**
BEGRENSET (lavgradert)		
KONFIDENSIELL		
HEMMELIG		
STRENGT HEMMELIG		

Informasjonsverdiene må sees i den sammenhengen og konteksten de er en del av, og ikke som en isolert enhet.

Når enhetene i virksomheten gjør verdivurderinger av egne aktiviteter og fellestjenester, vil disse vurderingene berike klassifisering av informasjonen som inngår i disse.

Ved å forstå betydningen av egne verdier i et større bilde, kan verdiene også få riktig beskyttelse.

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

4. Øvrige anbefalinger

Avslutningsvis kommer vi med noen øvrige anbefalinger som er viktige for arbeidet med verdioversikt.

4.1 Verdier og helhetlig sikkerhetsstyring

Ledelsen i virksomheten må involveres i arbeidet med verdioversikten. Det danner grunnlaget for god sikkerhetsstyring i dybden av kjernevirksomhet.

Kapittel 6[54] i **Styringsdokumentet for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor sier at**

«Informasjon behandles i et samspill mellom mennesker, prosesser og teknologi. Informasjonssikkerhet 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 del av det øvrige sikkerhetsarbeidet i virksomheten og skal inngå i den helhetlige virksomhetsstyringen. I kapittel 7, om sikkerhetsloven, beskrives det hvordan arbeidet med informasjonssikkerhet, forebyggende sikkerhetsarbeid og virksomhetsstyring kan samordnes.»

[55]

Vi vil understreke viktigheten av at det er ledernes ansvar at verdivurderinger gjennomføres, og følger opp sitt ansvar for at sikkerheten ivaretas der verdiene har beskyttelsesbehov.

Verdioversikten bør være kartlagt og systematisert i tråd med virksomheten sin organisering, og følge «lederlinjen». Det gir et godt grunnlag for virksomheten sitt systematiske sikkerhetsarbeid.

---

[54] Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor - regjeringen.no
[55] Hva vil det si å jobbe helhetlig? | Digdir

4.2 Gjennomfør risiko- og sårbarhetsanalyser

Denne veilederen har gitt en tilnærming til hvordan verdioversikt kan bygges. En slik verdioversikt er et nødvendig grunnlag for å finne frem til eventuell *skjermingsverdig* informasjon og informasjonssystemer etter sikkerhetsloven. Oversikten vil også være et viktig grunnlag for å etablere kontekst for overordnete ROS-analyser. ROS-analysen inneholder vurderinger av verdi, trussel, sårbarhet, og sannsynlighet og konsekvens, på et mer overordnet nivå enn hva risikovurderinger vanligvis gjør.

Kapittel 5[56] i Styringsdokumentet for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor sier at virksomhetene skal utarbeide ROS-analyser.

- «(…) utarbeide ROS-analyser som omfatter de tre sikkerhetsområdene samfunnssikkerhet og beredskap, nasjonal sikkerhet, og informasjonssikkerhet og personvern.»

Beredskapsrådet for kunnskapssektoren[57] har utarbeidet en nasjonal veileder for gjennomføring av risiko- og sårbarhetsanalysen (ROS-analysen). Veilederen sier at:

«ROS-analysen har som mål å kartlegge og vurdere risikoen knyttet til virksomhetens drift på et overordnet nivå, oppnå god risikoforståelse, og gi et underlag for valg av tiltak. I ROS-analysen identifiseres mulige hendelser og situasjoner som kan *true virksomhets verdier*. Gjennom å vurdere hva som kan skje og tilhørende usikkerhet, er det mulig å identifisere og iverksette relevante tiltak som kan bidra til å hindre at den aktuelle hendelsen inntreffer og/eller redusere konsekvensene dersom hendelsen ikke kan unngås»[58].

Beredskapsrådets veileder er utformet som et godt verktøy også for gjennomføring av ROS-analyse for uønskede hendelser innenfor de tre nevnte sikkerhetsområdene, over. Som del av planleggingen av ROS-analysen må det avklares hvilke verdier og konsekvenstyper som skal inkluderes i analysen.

En oversikt over virksomhetens verdier, er en del av forarbeidet til å gjennomføre denne typen nødvendige ROS-analyser.

[56] Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor - regjeringen.no
[57] Beredskapsrådet for kunnskapssektoren | Universitetet i Stavanger (uis.no)
[58] Veileder i risiko- og sårbarhetsanalyser for kunnskapssektoren | Universitetet i Stavanger (uis.no)

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim