Sikt
Kunnskapssektorens tjenesteleverandør

STYRINGSSYSTEM FOR SIKKERHET OG SIKKERHETSORGANISASJON

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

Formålet med denne veilederen er å bidra til mer klarhet i hvordan sikkerhetsarbeidet ved virksomhetene i norsk forskning og utdanning kan utformes og organiseres, iht. krav i kapittel 7 i Styringsdokument for arbeid med samfunnssikkerhet og beredskap i Kunnskapsdepartementets sektor[1].

Alle statlige, fylkeskommunale og kommunale organer er underlagt sikkerhetsloven[2], og skal dermed ha en dokumentert organisering og gjennomføring av sitt sikkerhetsarbeid[3].

Dette betyr at virksomhetene skal ha et styringssystem for sikkerhet med vedtatte mål og strategier, og med beskrivelse av hvilke roller med påfølgende ansvar som utgjør sikkerhetsorganisasjonen. Dersom virksomheten har verdier som er skjermingsverdige etter sikkerhetslovens bestemmelser[4], må sikkerhetsorganisasjonen også definere og begrunne hvilke roller som har behov for sikkerhetsklarering og autorisasjon.

Ifølge NSM sin Veileder i sikkerhetsstyring[5] skal sikkerhetsarbeidet være tilpasset og dimensjonert for de *verdier*, aktiviteter og tjenester i virksomheten som har beskyttelsesbehov. Verdioversikt og vurdering av betydning og kritikalitet til de ulike aktivitetene og tjenestene som virksomheten har, er derfor helt sentralt for å over tid bygge og opprettholde et tilstrekkelig sikkerhetsnivå.

Denne veilederen gir en kort innføring i hva et styringssystem for sikkerhet er, hvordan det kan utformes, og hvordan en sikkerhetsorganisasjon kan se ut.

Veilederen gir en inngang til sentrale momenter i materiell fra Nasjonal sikkerhetsmyndighet (NSM) og Digitaliseringsdirektoratet (Digdir). Veilederen presenterer anbefalinger som er basert på fra erfaringsdeling fra virksomhetene i forskning og utdanning.

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

---

[1] Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor - regjeringen.no
[2] https://lovdata.no/lov/2018-06-01-24/§1-2
[3] Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften) - Lovdata
[4] Lov om nasjonal sikkerhet (sikkerhetsloven) - Kapittel 4. Generelle krav til forebyggende sikkerhetsarbeid - Lovdata
[5] Sikkerhetsstyring - Nasjonal sikkerhetsmyndighet (nsm.no)

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

1. Styringssystem for sikkerhet

I Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor[6] står det i kapittel 7 at alle virksomhetene underlagt Kunnskapsdepartementet er omfattet av sikkerhetsloven. Det fremgår videre at virksomhetene skal ha et styringssystem for sikkerhet, som er samordnet ledelsessystemet for informasjonssikkerhet, øvrig virksomhetsstyring, og med en tydelig sikkerhetsorganisasjon. Styringssystemet for sikkerhet skal være avgrenset til HMS-systemet, som ivaretar liv og helse-aspektet.

Kravet om sikkerhetsstyring er utdypet i virksomhetssikkerhetsforskriftens kapittel 2 med krav om etablering av sikkerhetsstyringssystem i § 3[7]:

> *§ 3. Styringssystem for sikkerhet*
>
> *En virksomhet som omfattes av sikkerhetsloven, skal etablere et styringssystem for sikkerhet. Systemet skal sikre at virksomheten oppfyller kravene gitt i eller med hjemmel i loven.*

Les gjennom både sikkerhetsloven og virksomsikkerhetsforskriften for å bli nærmere kjent med bestemmelsene, og hvilke som vil gjelde for egen virksomhet.

1.2 Verdier er utgangspunktet

Sikkerhetsarbeidet er til for å sikre virksomhetens samfunnsoppdrag, kjernevirksomhet og alt som understøtter dette. Dette er mange lag med *verdier*. Verdiene understøtter virksomhetens leveranse- og utviklingsevne, og ivaretar mer overordnede konsekvenskategorier som økonomi, omdømme og kvalitet. Verdier er også funksjoner, prosesser eller 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. Verdivurdering av virksomheten, og av virksomhetens verdier er dermed grunnlaget for dimensjoneringen av sikkerhetsarbeidet.

Det kan være litt uklart for oss hvordan vi skal gå frem for å få verdioversikt. Dette kan komme av at verdiene er lagvise, de henger sammen, og vi har kanskje ikke definerte kriterier å vurdere dem ut ifra. Det er likevel et lovkrav å vurdere, kartlegge og holde oversikt over virksomhetens skjermingsverdige verdier[8]. Det er fordi enkelte virksomheter kan forvalte verdier som kan være av en viss betydning for nasjonale sikkerhetsinteresser[9], eller som regnes for å ha en samfunnskritisk funksjon[10]. En verdivurdering må derfor til for å avgjøre hvorvidt noe i virksomheten er skjermingsverdig. I de aller fleste tilfeller kommer man nok frem til at koblingen er lang[11] i forskning og utdanning, men vurderingen må likevel gjøres.

Sikkerhetsloven og virksomhetssikkerhetsforskriften gjelder uansett om virksomheten ikke har skjermingsverdige verdier, og verdioversikten er like fullt grunnleggende for sikkerhetsarbeidet[12]. NSM har veiledere og håndbøker [13]som støtter dette arbeidet, og som uansett gir godt grunnlag for metode og systematikk. *Les mer om verdier i eduCSC sin Veileder, Hva er verdioversikt. (lenke)*

---

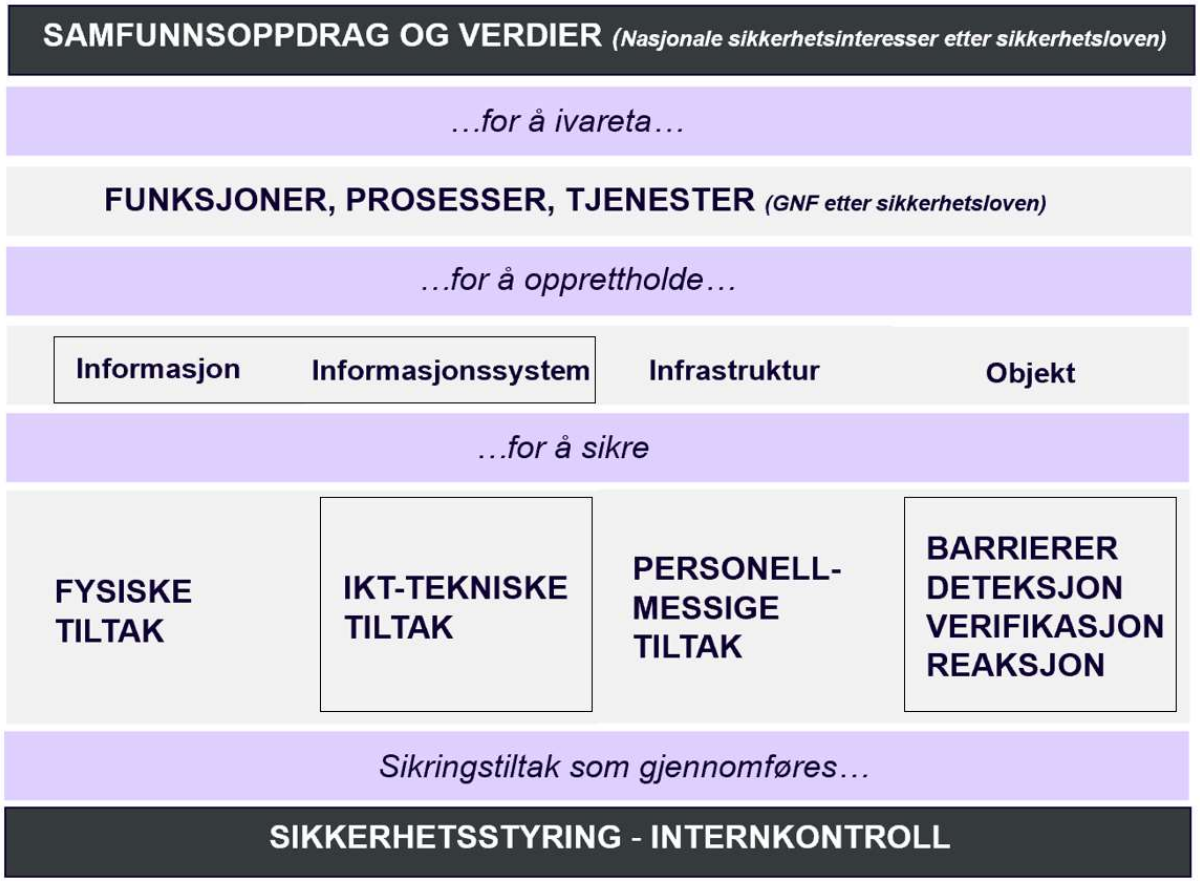
[6] Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor - regjeringen.no
[7] https://lovdata.no/forskrift/2018-12-20-2053/§3
[8] https://lovdata.no/forskrift/2018-12-20-2053/§2
[9] Nasjonale sikkerhetsinteresser - Nasjonal sikkerhetsmyndighet (nsm.no)
[10] Samfunnets kritiske funksjoner | Direktoratet for samfunnssikkerhet og beredskap (dsb.no)
[11] Skadefølger - Nasjonal sikkerhetsmyndighet (nsm.no)
[12] Informasjonssikkerhet for skjermingsverdige verdier etter sikkerhetsloven | Digdir
[13] Veiledere og håndbøker til sikkerhetsloven - Nasjonal sikkerhetsmyndighet (nsm.no)

1.3 Sikkerhetsstyringens formål

For å illustrere sikkerhetsstyringens formål, har vi bearbeidet 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 sitt overordnede bilde på egen verdioversikt som sikkerhetsarbeidet er til for. Videre har vi lagt en tynn ramme rundt de områdene som denne veilederen har hovedvekten sin på; informasjonssikkerheten.

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. Hvilke verdier som legges inn i de ulike «lagene» må virksomheten selv vurdere, ut fra sin kjernevirksomhet og overordnede verdioversikt.

Les modellen nedenfra og opp!



En virksomhet sin sikkerhetsstyring på dette området, foregår altså gjennom et styringssystem for sikkerhet. Et ledelsessystem for informasjonssikkerhet (LSIS/ISMS) har også samme formål, men kan være noe begrenset i omfang slik at det ikke dekker en helhetlig beskyttelse av alle verdiene.

I styringssystem for sikkerhet skal virksomheten beskrive sikkerhetsmål og strategier for sikkerhetsarbeidet, med definerte retningslinjer for de ulike områdene, og med en tydelig sikkerhetsorganisasjon.

1.4 Utdrag fra NSM sin Veileder i sikkerhetsstyring

Utformingen av sikkerhetsstyringssystemet avhenger av de verdier som skal beskyttes og hvordan beskyttelsen etableres. Et oppdatert trussel- og risikobilde er også viktig i utformingen og forbedringen av sikkerhetsstyringen. NSM legger til grunn at styringssystemet for sikkerhet skal omfatte hele det forebyggende sikkerhetsarbeidet, det vil si både aktiviteter dedikert til sikkerhet og aktiviteter som kan ha betydning for sikkerhet. Dette innebærer at styringssystemet for sikkerhet skal omfatte:

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

Styringssystemet for sikkerhet skal samordnes med virksomhetsstyringen for øvrig. Dette vil gi grunnlag for felles tilnærming i håndteringen av de risikoer virksomheten står overfor. Ved samordning er det viktig å være oppmerksom på at sikkerhetsarbeidet vil kunne medføre behandling av skjermingsverdig informasjon[14].

15

Sikkerhetsstyringen med sikringstiltak er et kontinuerlig arbeid. Det vil ikke alene kunne foregå som én sentralt styrt, lineær prosess, men som mange lokale og sirkulære prosesser. Et styringssystem for sikkerhet som fungerer i organisasjonen kjennetegnes ved at lederlinjen og de ansatte har et forhold til sine verdier og verdienes betydning, hvilke lovkrav som gjelder, og hva som truer verdiene. Virksomheten og enhetene er klar over hvordan de selv er sårbare, og har forebyggende tiltak.

Virksomheten må be enhetene om periodevis rapportering på sikkerhetsarbeidet, på samme måte som for økonomi, HMS, og andre internkontrollområder.

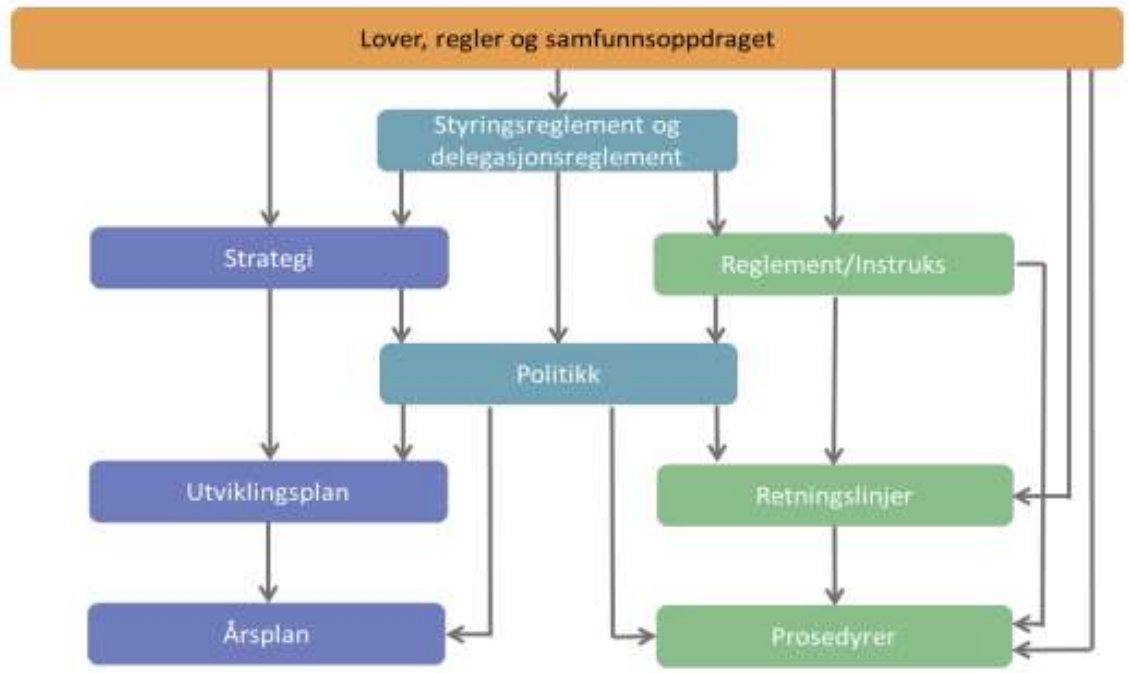
[14] Om denne veilederen - Nasjonal sikkerhetsmyndighet (nsm.no)
[15] Hva vil det si å jobbe helhetlig? | Digdir

1.5 Anbefalinger til utforming av styringssystem for sikkerhet

1.5.1 Gjør sikkerhetsstyringen til en del av virksomhetsstyringen

Et helhetlig styringssystem for sikkerhet bør henge sammen med *dokumenthierarkiet* på tvers av andre internkontrollområder, og ikke minst til virksomhetsstrategier og mål. Kravene til sikkerhet må være mulige å forstå og etterleve for alle med et ansvar i organisasjonen

Hvordan dette er skrudd sammen ved de ulike virksomhetene er trolig ulikt. Her er et eksempel på hvordan et dokumenthierarki for styring og delegasjon ved et av landets universiteter er illustrert:



[16]

For at sikkerhetsstyring skal innlemmes i øvrig virksomhetsstyring, og for å få til god virksomhetstilpassing, er det derfor best å ikke starte helt fra bunn. Se til hvilke interne styringssystemer eller ledelsessystemer virksomheten allerede har når sikkerhetsstyring etter sikkerhetsloven skal utformes eller videreutvikles. Husk også at ikke alt må komme på plass med det samme.

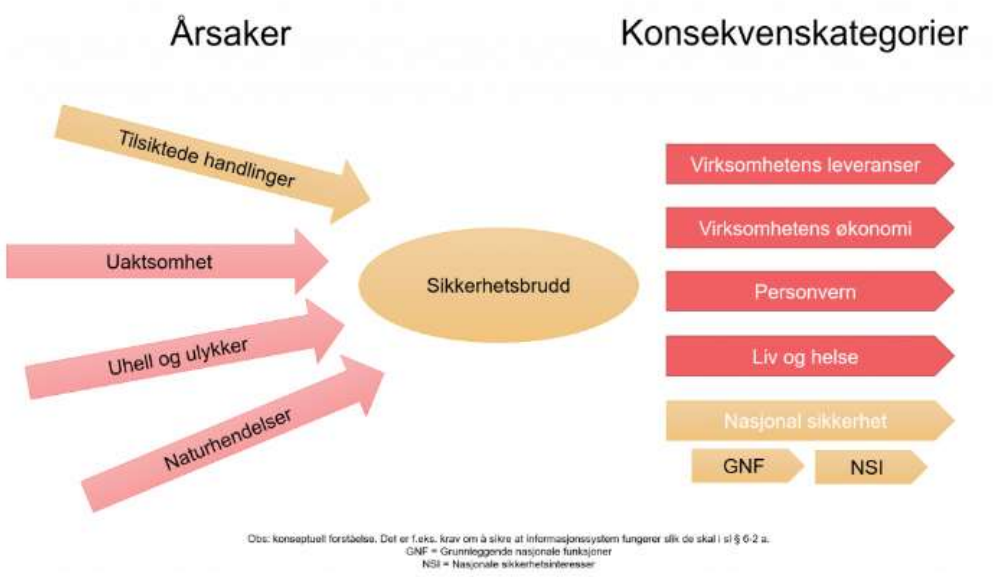
Undersøk og vurder følgende:

- *Hvordan foregår virksomhetsstyringen hos oss?*
- *Hvilke styrende dokumenter har vi, til hvilke formål?*
- *Hva mangler vi for å dekke krav til sikkerhetsstyring hos oss?*
- *Hva skal vi starte med?*

De fleste virksomheter har utformet styrende dokumenter for ulike internkontrollområder. Disse internkontrollområdene dekker forvaltningsområder som er gjenstand for andre lovkrav for internkontroll enn hva som direkte følger av sikkerhetsloven og virksomhetssikkerhetsforskriften. HMS-arbeidet følger for eksempel krav gitt av internkontrollforskriften og arbeidsmiljøloven. Arbeidet med informasjonssikkerhet og personvern er eksempelvis forankret både i e-forvaltningsforskriften og

[16] Styringsreglement - Kunnskapsbasen - NTNU

personopplysningsloven. Beredskapsarbeidet følger av samfunnssikkerhetsinstruksen og skal gjøre virksomheten i stand til å håndtere enhver hendelse som mobiliserer kriseledelsen, enten hendelsen er ulykke, en større omdømmesak eller overlagte sikkerhetshendelser.



17

Gjennom å se på eksisterende styrende dokumenter kan det finnes gode rettesnorer for hvordan også sikkerhetsstyringen bør ta form, og hvordan roller og ansvar bør fordeles. Politikk-dokumenter kan ofte ha en tilnærming til en mer *mål-orientert* risikostyring og internkontroll, og omtaler kanskje i mindre grad *hvilke verdier* virksomheten forvalter og hvilke beskyttelsesbehov de har ut fra *tilsiktede handlinger*. Det er derfor ofte nødvendig at virksomheten stadfester og vedtar en egen politikk for sikkerhet, til nettopp dette formålet.

Dette er også hjemlet i virksomhetssikkerhetsforskriften kap. 2, § 4[18]:

> *§ 4, Styringsdokument for det forebyggende sikkerhetsarbeidet*
>
> *Lederen for en virksomhet skal fastsette et styringsdokument som beskriver*
>
> *a. Hvilke deler av sikkerhetsloven med forskrifter som gjelder for virksomheten*
> *b. Roller og ansvar i virksomhetens forebyggende sikkerhetsarbeid, jf. § 6*
> *c. Prinsipper for virksomheten sikkerhetsarbeid*

Et styringsdokument for det forebyggende sikkerhetsarbeidet, eller en *politikk for sikkerhet,* bør stadfeste virksomhetens samfunnsoppdrag, og overordnet hvilke verdier som forvaltes. Her kan det for eksempel henvises til kjernevirksomhet som forskning, utdanning, formidling, nyskaping, og støttefunksjoner. En kan også legge til hvorvidt virksomheten har særlig profilerte fagmiljøer, som har stor betydning for virksomheten, og dermed for sikkerhetsarbeidet.

Videre skal politikken stadfeste overordnede sikkerhetsmål, med strategier og prinsipper for sikkerhetsarbeidet. Politikken skal også inneholde hvilke roller med tilhørende ansvar som inngår i sikkerhetsorganisasjonen.

---

17 Informasjonssikkerhet for skjermingsverdige verdier etter sikkerhetsloven | Digdir
18 https://lovdata.no/forskrift/2018-12-20-2053/§4

1.5.2 Gjør sikkerhetsstyringen og arbeidet med informasjonssikkerhet til samme «system»

Mange av verdiene i forskning og utdanning omfatter kunnskap og informasjon, informasjonsteknologi- og systemer, og utviklings- og innovasjonsprosesser. Mange prosesser og støttetjenester er digitalisert. De fleste virksomheter har innført ledelsessystem for informasjonssikkerhet, etter gjeldende styringsmodell[19]. Det kan derfor være en god tilnærming at styringssystemet for sikkerhet utvider og forsterker virksomhetens allerede etablerte ledelsessystem for informasjonssikkerhet.

Som hjelp i arbeidet kan det sees til anbefalt rammeverk for ledelsessystem for informasjonssikkerhet, ISO/IEC 27001:2013 [20]eller nyere. ISO/IEC 27002:2023 omfatter tiltaksområder og medfølgende kontrollpunkter som vil gi god dekning av sikkerhetsarbeidet. NSM sine grunnprinsipper[21] gir også et svært godt og helthetlig grunnlag, og bør i det minste benyttes som et supplement til ISO.

Politikk for sikkerhet vil måtte ha *underliggende prosedyrer* eller retningslinjer for de mer spesifikke områdene av sikkerhetsarbeidet. Disse skal tydeliggjøre ansvaret for styringsaktivitetene og sikkerhetstiltakene i hele bredden. Ansvaret bør fordeles slik det er hensiktsmessig i organisasjonen, og gjenspeile sikkerhetsorganisasjonen.

Noen virksomheter har all styringsinformasjon i ett og samme dokument. Andre deler opp i enkeltdokumenter. Det anbefales at styringsdokumenter følger en lik mal og struktur i hele virksomheten, og at de merkes med versjonshistorikk, gyldighet, og hvem som er ansvarlig.

Aktuelle prosedyrer i et styringssystem for sikkerhet, som også dekker informasjonssikkerhet i en virksomhet, kan være prosedyre/retningslinje for -

- *Risikostyring (med verdivurdering, risikovurdering og tiltak)*
- *Behandling av personopplysninger (personvern er ofte en del informasjonssikkerhet)*
- *Kontroll med kunnskapsoverføring/Eksportkontroll (dersom aktuelt)*
- *Teknisk grunnsikring (kan være behov for flere her)*
- *Objektsikkerhet, fysisk sikring og adgangskontroll*
- *Tilgangsstyring*
- *Anskaffelser og leverandørkontroll*
- *Opplæring og arbeid med sikkerhetskultur (Personellsikkerhet)*
- *Håndtering av avvik og sikkerhetshendelser*
- *Kontroll og forbedring (internkontroll)*
- *Personellsikkerhet og autorisasjon (obligatorisk for behandling av informasjon gradert etter Sikkerhetsloven og/eller tilkobling til Nasjonalt BEGRENSET nett)*
- *Prosedyre for sikring av beskyttet område (obligatorisk for tilkobling til Nasjonalt BEGRENSET nett)*

(Listen er ikke fullstendig, og er kun eksempler)

En politikk for sikkerhet og underliggende prosedyrer eller retningslinjer må vedtas etter gjeldende styrings- og delegasjonsreglement. Det anbefales å forankre arbeidet med styringssystem for sikkerhet i øverste ledelse, og sørge for å involvere relevante ressurser og nøkkelpersoner. Videre bør det lages en plan for implementering. Det er også viktig å påpeke at selve gjennomføringen og etterlevelsen av kravene i sikkerhetsstyringen vil best kunne foregå som en del av alle aktiviteter, prosesser og tjenester som utføres i det daglige. Dersom sikkerhet blir en aktivitet «på siden», blir arbeidet både tyngre og mer kostbart i tids- og ressursbruk.

---

[19] F-04-20 Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning - regjeringen.no
[20] NS-EN ISO/IEC 27001 Informasjonssikkerhet - Krav | standard.no
[21] Råd og anbefalinger - Nasjonal sikkerhetsmyndighet (nsm.no)

1.5.3 Gjennomfør helhetlige styringsaktiviteter og sikkerhetstiltak

Digdir sin veileder i helhetlig sikkerhetsarbeid[22] sier at med et helhetlig styringssystem for sikkerhet har virksomheten etablert styringsaktiviteter med klare roller, ansvar og rapporteringslinjer. Dette er ledelsens redskap for å følge opp og styre arbeidet med sikkerhet. Virksomheter som evner å arbeide helhetlig, har en toppledelse som følger opp styringsaktivitetene på tvers av fagområder.

[23]

Sikkerhetsarbeidet må i tillegg være effektivt, og la seg gjennomføre med tilgjengelige ressurser. Styringsaktivitetene bør derfor fungere på tvers av fagområder og på tvers av prosesser og aktiviteter i virksomheten. Det vil likevel være ulike metoder i bruk, og forskjellige måter å gjennomføre deler av aktivitetene på, alt etter hvilke hensyn som skal ivaretas og hvilke regelverk som gir føringer for de ulike enhetene i virksomhetens kjernevirksomhet.

Tenk tilbake til den overordnede verdioversikten, og tenk på behovet for ulike sikkerhetstiltak.

- *Noen enheter forsker på biologisk materiale, helsedata og personopplysninger*
- *Noen enheter administrerer skikkethetsvurderinger for psykologistudenter*
- *Noen enheter forsker på teknologi som kan ha nytteverdi for militære formål*
- *Noen enheter bruker svært avansert og kostbart laboratorieutstyr*
- *Noen enheter utreder utfordrende personalsaker og arbeidsmiljøkonflikter*

Noen sikkerhetstiltak vil gjelde for hele virksomheten. Samtidig vil det være miljøer og enheter som har aktiviteter som fordrer særlige tiltak. Et helhetlig styringssystem for sikkerhet må legge til rette for at de riktige styringsaktivitetene og sikkerhetstiltakene også kan besluttes og iverksettes lokalt, ut fra de beskyttelsesbehov som er nødvendige. Ledelsen skal over tid kunne bygge en tilstrekkelig oversikt over det totale sikkerhetsarbeidet gjennom de etablerte rapporteringslinjene og den interne styringsdialogen. Målet må være å holde riktig balanse mellom åpenhet og risiko!

[22] Hva vil det si å jobbe helhetlig? | Digdir
[23] Hva vil det si å jobbe helhetlig? | Digdir

2. Sikkerhetsorganisasjon, roller og ansvar

Virksomhetssikkerhetsforskriften har krav om fordeling av ansvar og myndighet for roller i det forebyggende sikkerhetsarbeidet i § 6[24]:

§ 6. Roller i og ansvar for det forebyggende sikkerhetsarbeidet (første og tredje ledd)

Lederen for en virksomhet skal fordele roller i og ansvar for det forebyggende sikkerhetsarbeidet, slik at kravene gitt i eller med hjemmel i sikkerhetsloven ivaretas. Rollene og ansvarsfordelingen skal gjøres kjent i virksomheten.

Kontrollen av styringssystemet for sikkerhet skal om mulig utføres av andre enn de som har styrende eller utøvende oppgaver i det forebyggende sikkerhetsarbeidet

2.1 Utdrag fra NSM sin Veileder i sikkerhetsstyring

Forebyggende sikkerhetsarbeid vil omfatte aktiviteter knyttet til beslutninger, utførelse og oppfølging. Ansvar og myndighet for disse aktivitetene må være fordelt til rollene som skal gjennomføre dem. Virksomhetens ledelse beslutter overordnede føringer for forebyggende sikkerhetsarbeid og følger opp arbeidet. Linjeledere er ansvarlig for sikkerhetsarbeidet innen sitt myndighetsområde og hver medarbeider har ansvar for at egen arbeidsutførelse er sikker og som besluttet. I tillegg kan virksomheten utpeke enkelte roller med dedikerte oppgaver i det forbyggende sikkerhetsarbeidet.

Antall og typer roller som etableres må sees i sammenheng med de (skjermingsverdige) verdiene virksomheten råder over og omfanget av disse. Som minimum er det aktuelt å fordele ansvar og myndighet for å følge opp og bistå det forebyggende sikkerhetsarbeidet til roller som bistår ved, og påser gjennomføring av arbeidsoppgaver med betydning for sikkerhet. Eksempelvis kan det være behov for funksjonen *sikkerhetsleder* til å koordinere og lede dette arbeidet. Utførelse av forebyggende sikkerhetsarbeid, og oppfølging av dette arbeidet må skje uavhengig av hverandre, blant annet slik at ikke medarbeidere settes til å kontrollere egen arbeidsutførelse[25].

NSM sin veileder i sikkerhetsstyring sier også at virksomheter med utstrakt bruk av informasjonsteknologi også kan ha behov for en *IKT-sikkerhetsleder*. Dette kan sies å gjelde for virksomheter innen forskning og utdanning. I dag har de fleste gjerne en *CISO (Chief information security officer)* eller lignende funksjon som følger opp ledelsessystemet for informasjonssikkerhet. Mange virksomheter har i tillegg fordelt ansvaret for gjennomføringen av de IKT-tekniske sikkerhetskravene til IT-avdelingen eller til en IT-sikkerhetsleder.

Når den helhetlige sikkerhetsorganisasjonen skal tegnes er det viktig med en riktig tilpasning til, og utvidelse av, det etablerte informasjonssikkerhetsarbeidet med tilhørende roller og ansvarsområder. Se også til andre beslektede internkontrollområder, og organiseringen av arbeidet.

[24] https://lovdata.no/forskrift/2018-12-20-2053/§6
[25] Roller i det forebyggende sikkerhetsarbeidet - Nasjonal sikkerhetsmyndighet (nsm.no)

2.2 Anbefalinger til organisering av sikkerhetsarbeidet

Når roller og ansvar skal fordeles i en helthetlig sikkerhetsorganisasjon, vil det være fornuftig å tilpasse til den eksisterende organiseringen av annet internkontrollarbeid, og til de ressurser og den kompetanse som virksomheten allerede besitter. Dette skal selvsagt også henge sammen med de styrende dokumentene i styringssystemet. Gjør så en vurdering av hvilke roller virksomheten mangler for å få de rollene som sikkerhetsloven krever. Dersom virksomheten har skjermingsverdige verdier, eller skal kunne motta og svare på gradert eller lavgradert informasjon, kreves også roller som ivaretar autorisasjon av personell, og en utpeking av hvem som skal autoriseres, til hvilket formål. Dersom det er usikkert hvorvidt dette er nødvendig hos seg, er det greit å vente med disse rollene.

2.2.1 Se på eksisterende roller i virksomheten sine styrende dokumenter

Ta først en gjennomgang av hvilke roller, funksjoner og ansvarsområder virksomheten allerede har etablert for beslektede internkontrollområder, og særlig for arbeidet med informasjonssikkerhet. Her kan det være gode muligheter for å bevare og bygge ut enkelte roller, fremfor å starte fra bunn.

Tabellen under er eksempler på hvordan roller og ansvar ofte er fordelt på innenfor noen beslektede internkontrollområder.

Teksten i kursiv er kun som enkle eksempel, og er ikke ment som til etterfølgelse!

Rolle	Politikk for risikostyring	Politikk for internkontroll	Politikk for informasjons-sikkerhet	Politikk for personvern
Rektor/ Direktør	*Har det overordnede ansvaret for at virksomheten har etablert risikostyring og skal påse at risikostyringen gjennomføres som del av ordinær virksomhetsstyring.*	*Er ansvarlig for å påse at virksomheten til enhver tid har et effektivt internkontrollsystem. Dette innebærer at (…)*	*Er ansvarlig for at virksomheten har et styringssystem for informasjonssikkerhet med klare definerte roller, ansvar og rapporteringsveier i organisasjonen.*	*Har det overordnede ansvaret for behandling av personopplysninger i virksomheten, herunder virksomhetens rolle som hhv. behandlingsansvarlig eller databehandler (…)*
Prodekan/ Dekan/ Avdelings-direktør	*Har ansvar for at det blir identifisert og vurdert risikoer innenfor eget fakultet/divisjon/avdeling og at det blir iverksatt tiltak basert på divisjonens/avdelingens risikoer.*	*Er ansvarlig for å påse at internkontroll innen eget fakultet/divisjon/avdeling er etablert, dokumentert, gjennomført og fulgt opp på en systematisk og hensiktsmessig måte, (…)*	*Er ansvarlig for å implementere kravene til informasjonssikkerhet i eget virksomhetsområde. Ansvaret følger linjen.*	*Ansvarlig for å implementere personvernpolicyen på fakultets-/avdelingsnivå (…)*
Lederlinjen ***Instituttleder Seksjons-leder Enhetsleder***	*Har ansvar for at aktuelle aktiviteter ved institutt/prosjekt/tjeneste blir risikovurdert og at det blir gjennomført kontrollaktiviteter gjennom hele prosjektperioden/året.*	*Er ansvarlig for å implementere tilstrekkelige kontroller og andre risikoreduserende tiltak i egen enhet for å sikre målrettet og effektiv drift, pålitelig rapportering og overholdelse av lover og regler (…)*	*Ansvaret følger linjen. Risikoeier skal ha oversikt over egne verdier, hva som truer dem og hvilke sårbarheter som er ved egen enhet, for å avdekke og håndtere risiko.*	*Ansvarlig for å implementere personvernpolicyen på insitutt-seksjons- eller prosjektnivå (…)*
Risikoeier ***Leder Prosjektleder Forsknings-leder …***	*Har ansvar og myndighet til å sørge for at risikoreduserende tiltak blir fulgt opp. Risikoeierskap skal følge linjen.*		*Risikoeier skal ha oversikt over egne verdier, hva som truer dem og hvilke sårbarheter som er ved eget aktivitetsområde, for å avdekke og håndtere risiko.*	
Fag-spesifikke roller innen Brannvern og Fysisk sikring				

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

Riskmanager	*Alle større risikovurderinger ledes av en fasilitator. Fasilitator forklarer metode/prosess for deltakerne, styrer diskusjoner og tidsbruk, stiller spørsmål om årsaker til risiko og påser at mal for risikovurderinger fylles ut på alle punkter.*			
Fagansvarlig internkontroll (og eventuelt direktør for Virksomhets-styring)	*Skal bistå ledergrupper i overordnede risikovurdering. Funksjonen har også ansvar for at malverk oppdateres og bistår med at gjennomførte risikovurderinger lagres på riktig område.*	*Er ansvarlig for å bistå ledelsen med å koordinere, utvikle og vedlikeholde internkontrollsystemet (…)*		
Sikkerhets-leder / Beredskaps-koordinator			*Er utøvende for at virksomheten jobber systematisk med beredskap og kontinuitet for informasjons-sikkerhetshendelser som del av virksomhetens planverk.*	
CISO			*Er ansvarlig for å utvikle og bekjentgjøre den operative oppfølging av informasjons-sikkerhetsarbeidet, i tillegg til å sette strategiske mål for sikkerheten. (…)*	
Systemeier / SYstemforvalter				
Personvern-ombud				*Gi råd og veiledning om GDPR og personopplysningsloven til ansatte (…)*
Sikkerhets-respons-teamet (IRT)			*Skal håndtere brudd/hendelser innen informasjonssikkerhet*	*Følge opp avvik på personopplysningssikkerheten i henhold til prosedyre for brudd på informasjonssikkerheten.*

Ikke glem beredskapsprinsippene Ansvar – Likhet – Nærhet – Samvirke når sikkerhetsorganisasjonen utvikles.

Likhetsprinsippet sier at den organisasjon man operer med under kriser skal i utgangspunktet være mest mulig lik den organisasjon man har til daglig.

Se også derfor til roller og ansvar i virksomhetens beredskapsorganisasjon.

2.2.2 Vurder hvilke roller som mangler

For å etablere en komplett sikkerhetsorganisasjon etter gjeldende lovkrav, må enkelte roller som for eksempel *sikkerhetsleder*, *datasikkerhetsleder* og eventuelt rollen som *autorisasjonsansvarlig* være fordelt. Hvordan disse rollene faktisk gjør seg gjeldende og må være en del av sikkerhetsorganisasjonen, kommer an på sikringsbehovet til virksomhetens verdier. Verdioversikten må vise hva virksomheten selv vurderer å være av betydning. Verdier som er skjermingsverdig, medfører særlige sikringstiltak og også særskilte roller i sikkerhetsorganisasjonen.

Dersom virksomheten ikke har en slik overordnet verdioversikt, er det helt greit å ta utgangspunkt i den oversikten og de vurderinger man eventuelt har, av kjernevirksomheten med alle støttetjenester.

Roller kan legges til i sikkerhetsorganisasjonen etter hvert som også verdioversikten utvides.

Dette er helt i tråd med at sikkerhetsarbeidet skal være i kontinuerlig utvikling og forbedring.

Tydeliggjør roller som kan overlappe
Ved å se på de roller som allerede er i virksomhetens interkontroll-systemer, og skal vurdere hva som mangler, kan navn på roller av og til skape forvirring. Et eksempel er funksjonen *CISO (Chief Information Security Officer)*. Denne rollen kan også fungere eller omtales som en *datasikkerhetsleder* eller *IT-sikkerhetsleder*. En IT-leder kan også ha ansvaret som IT-sikkerhetsleder eller datasikkerhetsleder. Et annet eksempel er funksjonen *beredskapskoordinator*, *sikkerhetsrådgiver*, *sikkerhetsleder*, eller lignende. Her kan det være duket for rolleuklarhet og overlapp, noe som vil kunne skape usikkerhet og utfordringer både i det forebyggende sikkerhetsarbeidet og når hendelser skjer.

Det er viktig at roller og ansvar er tydelige og avgrenset til hverandre, og ikke overlapper eller blir uklare. Tydeliggjør de rollene som kanskje allerede utøves i praksis i dag, og formaliser dem i sikkerhetsorganisasjonen. Det er viktig å bevare det som fungerer, selv om det ikke har vært beskrevet og forankret tidligere.

Sikkerhetsloven gir rom for fleksibilitet og virksomhetstilpasning. Finn den fordelingen som passer best med de ressurser og den kompetanse virksomheten har.

Vurder behovet for lokale roller i sikkerhetsorganisasjonen
En overordnet verdioversikt skal gi svar på hvorvidt det er enheter, miljø eller funksjoner som har særlige sikringsbehov. Dersom det er tilfellet, kan det være fornuftig at det etableres lokale roller i sikkerhetsorganisasjonen som skal følge opp dette sikringsbehovet. Eksempel på mer fagspesifikke sikkerhetsroller, kan være rollen som lokal eksportkontroll-rådgiver, lokal personvernrådgiver, eller lokal rådgiver innen fysisk sikring.

Vurder behovet for informasjonsutveksling over sikkerhetsgraderte plattformer
Virksomheten *kan ha* behov for å kunne ta imot og svare på informasjon med andre over Nasjonalt BEGRENSET nett (NBN)[26]. NBN er utviklet av Forsvarsdepartementet for behandling av lavgradert informasjon[27] i statsforvaltningen. Denne tilkoblingen krever blant annet at virksomheten har prosessen for autorisasjon av en del nøkkelpersonell på plass. Det kreves også en del tiltak innen fysisk sikring og adgangskontroll.

Vurder behovet for rollen som autorisasjonsansvarlig
Rollen som *autorisasjonsansvarlig* er nødvendig for å ivareta prosessen med å få autorisert personell som får sikkerhetsklarering[28] for å blant annet kunne behandle gradert og lavgradert informasjon i virksomheten. Klareringsforskriften § 3 sier at autorisasjonsansvarlig i virksomheter som er underlagt sikkerhetsloven, kan be klareringsmyndigheten om klarering av nødvendige personer[29].

Sikkerhetsloven §§ 8 og 9 sier at *virksomhetens leder er autorisasjonsansvarlig* og har ansvaret for sikkerhetsmessig ledelse og kontroll av autoriserte personer[30]. Autorisasjonsansvarlig er ansvarlig for å autorisere personell for tilgang til sikkerhetsgradert informasjon. Den enkelte virksomhets leder kan, dersom behovet tilsier det, delegere autorisasjonsansvaret[31].

---

[26] Prop. 1 S (2015–2016) - regjeringen.no
[27] Sikkerhetsgraden BEGRENSET - Nasjonal sikkerhetsmyndighet (nsm.no)
[28] Sikkerhetsklarering - Nasjonal sikkerhetsmyndighet (nsm.no)
[29] https://lovdata.no/LTI/forskrift/2018-12-20-2054/§3
[30] https://lovdata.no/lov/2018-06-01-24/§8-9
[31] Autorisasjon - Nasjonal sikkerhetsmyndighet (nsm.no)

Vurder tjenstlig behov i virksomheten
Kjernevirksomheten i kunnskapssektoren omfatter som hovedregel ikke tilvirking av informasjon eller drift av infrastruktur og objekter som er av betydning for nasjonale sikkerhetsinteresser, og dermed vurderes til å være skjermingsverdig. Det kan likevel være unntak.

Funksjoner i virksomhetens operative sikkerhetsmiljø kan besitte informasjon eller ha tilgang til informasjon som gjennom analyse og sammenstilling *kan ha* betydning for nasjonale sikkerhetsinteresser. Slikt personell kan også samvirke eksempelvis med sitt sektorvise responsmiljø (eduCSC[32]), med Nasjonalt cybersikkerhetssenter (NCSC[33]), eller ha kontaktpunkter mot andre nasjonale sikkerhetstjenester. Med sikkerhetsklarering vil slikt personell kunne motta gradert informasjon på eksempelvis K og H. Sikkerhetsgradert informasjon vil som hovedregel ikke være aktuell for videre deling internt i virksomheten. De fleste ressurser i et operativt sikkerhetsmiljø vil også trolig være tilstrekkelig klarert med BEGRENSET (B) gjennom autorisasjonssamtale.

Funksjoner i virksomhetens øvrige sikkerhetsorganisasjon, og enkelte leder- og nøkkelpersoner kan også ha behov for sikkerhetsklarering og autorisasjon på ulike nivå for å kunne *motta* og behandle lavgradert og gradert informasjon. Tjenstlig behov[34] begrunnes i ansvaret for å kunne ivareta sikkerheten og kontinuiteten i sine områder av kjernevirksomheten, og for å kunne håndtere eventuelle større sikkerhetshendelser som berører virksomheten.

Merk at det også følger med en rekke krav til blant annet fysiske lokaler og adgangskontroll dersom virksomheten skal behandle skjermingsverdig informasjon[35].

2.2.3 Fordel roller i virksomhetens sin helhetlige sikkerhetsorganisasjon

En generell beskrivelse av forslag til fordeling av roller og ansvar for en virksomhet er følgende, hvor roller markert i grønt *vil kunne ha* behov for sikkerhetsklarering og autorisasjon:

Rolle	Ansvar
Rektor/Direktør	*Ansvarlig for at virksomheten har et styringssystem for sikkerhet, med fordelte roller og ansvar for det forebyggende sikkerhetsarbeidet, slik at kravene gitt i eller med hjemmel i sikkerhetsloven ivaretas.*
Sikkerhetsleder og/ eller Beredskapsleder *(kan også gjerne være autorisasjonsansvarlig)* *(Kan gjerne være en leder av en seksjon eller enhet for sikkerhet og kvalitet, eller lignende)* *(Sikkerhetsleder er en obligatorisk rolle dersom*	*Ansvarlig for at de styrende dokumenter for virksomheten sitt sikkerhetsarbeid er oppdatert, dekkende og holder et riktig nivå.* *Skal være prosessdriver for at virksomheten får overordnet verdioversikt.* *Skal også påse at de som har særlig ansvar for å gjennomføre sikkerhetskravene får informasjon og nødvendig opplæring.*

[32] Varsle om sikkerhetshendelser (sikt.no)
[33] Kontakt NCSC - Nasjonal sikkerhetsmyndighet (nsm.no)
[34] § 8-1 Krav om sikkerhetsklarering, adgangsklarering og autorisasjon - Nasjonal sikkerhetsmyndighet (nsm.no)
[35] Fysisk sikring - Nasjonal sikkerhetsmyndighet (nsm.no)

virksomheten skal ha tilkobling til Nasjonalt BEGRENSET nett)	*Er ansvarlig for å gi virksomhetsledelsen oppdatert risikobilde, og holde ledelsens gjennomgang.*
Beredskapsleder *(dersom denne rollen ikke er slått sammen med sikkerhetsleder)* *(Kan gjerne være en del av en seksjon eller enhet for sikkerhet og kvalitet, eller lignende)*	*Ansvarlig for virksomhetens systematiske arbeid med beredskap.* *Skal være prosessdriver for at virksomheten gjennomfører og oppdaterer risiko- og sårbarhetsanalyser, som skal ligge til grunn for utforming av beredskapsplaner.* *Skal være prosessdriver for gjennomføring av beredskapsøvelser, og at alle med roller vet hva de skal gjøre i en beredskapshendelse/krise.*
Informasjonssikkerhetsleder (CISO) *(Kan gjerne være en del av en seksjon eller enhet for sikkerhet og kvalitet, eller lignende)*	*Ansvarlig for styrende dokumenter som gjelder forvaltning og sikring av virksomheten sine informasjonsverdier (…)*
Datasikkerhetsleder *(Obligatorisk rolle dersom virksomheten skal ha tilkobling til Nasjonalt BEGRENSET nett)* *(Kan gjerne være tillagt IT-leder, eller en IT-sikkerhetsleder, eller CISO)*	*Ansvarlig for at virksomhetens IKT-infrastruktur holder et forsvarlig sikkerhetsnivå.*
Autorisasjonsansvarlig *(Kan gjerne også være sikkerhetsleder)* *(Kan gjerne være en del av en seksjon eller enhet for sikkerhet og kvalitet, eller lignende.* *Rollen bør ikke ligge i en HR-avdeling)*	*Autorisasjonsansvarlig er ansvarlig for å autorisere personell for tilgang til sikkerhetsgradert informasjon, samt følge opp autorisert personell. Ansvaret skal være skriftlig delegert av virksomhetens øverste leder.*
Incident Response Team (IRT)/ **SOC-team** *Behovet for sikkerhetsklarering og autorisasjon må vurderes på bekgrunn av verdiene og tjenstlig behov.*	*Være virksomheten sin operative vaktstyrke for å overvåke, oppdage og håndtere IKT-sikkerhetshendelser, og for tett dialog med sektorvist responsmiljø i eduCSC.*

Dekan/Divisjons/-Avdelings-direktør *Behovet for sikkerhetsklarering og autorisasjon må vurderes på bekgrunn av verdiene og tjenstlig behov.*	*Ansvarlig for å etterkomme virksomheten sine sikkerhetskrav innenfor sitt virksomhetsområde, og at tjenestene holder riktig sikkerhetsnivå.*
Instituttleder/Seksjonsleder/ Prosjektleder *Behovet for sikkerhetsklarering og autorisasjon må vurderes på bekgrunn av verdiene og tjenstlig behov.*	*Ansvarlig for å etterkomme virksomheten sine sikkerhetskrav innenfor sitt virksomhetsområde, og at tjenestene holder riktig sikkerhetsnivå.*
Avdelingsdirektør Virksomhetsstyring	*Ansvarlig for at det gjennomføres internkontroll av sikkerhetsarbeidet, for å påse at styringssystemet for sikkerhet fungerer.*
Ansatte	*Ansvarlig for å etterkomme virksomheten sine sikkerhetskrav innenfor sitt arbeidsområde, og bidra til en god sikkerhetskultur.*

3. Øvrige anbefalinger

3.1 Gi sikkerhet og beredskap riktig plassering i virksomheten

Alle som inngår i sikkerhetsorganisasjonen, vil naturlig nok være spredt i ulike deler av virksomheten. De færreste har sikkerhet og beredskap som sitt eneste arbeidsområde, med noen få unntak. Personvernombud, CISO, sikkerhetsleder, beredskapsleder, og tilsvarende, vil være eksempler på roller som har sikkerhet og beredskap som sitt hovedoppdrag.

Dette er ofte roller som har kommet inn i virksomheten over tid, og som er plassert i ulike deler av virksomheten. Dermed rapporterer de ofte også til ulike ledere. Dette kan være til hinder for et robust og helhetlig sikkerhetsarbeid.

Ved å samle de rollene som koordinerer og driver arbeidet med sikkerhet og beredskap på virksomhetsnivå i samme enhet, får de én rapporteringslinje som vil gi mer kraft til arbeidet. Når de sentrale rollene er samlet, legges forholdene til rette for bedre overlapp og samstyring av de ulike sikkerhetsområdene sine styringsaktiviteter og sikkerhetstiltak i virksomheten.

Hva som er riktig plassering i virksomheten kan være ulikt, og avhengig av virksomhetens organisering av de øvrige fellesadministrative støttetjenester og internkontrollområder.

Husk at IT og IKT står for informasjonsteknologi og informasjons- og kommunikasjonsteknologi.

Husk at HR står for human resources.

Husk HMS handler om liv og helse.

Husk at sikkerhet og beredskap går på tvers av alle aktiviteter og prosesser, og handler om virksomhetsstyring, ledelse og kvalitet.

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

3.2 Gi rom for flere perspektiver og ulike kompetanser

Et helhetlig sikkerhetsarbeid krever ulike roller og ulike kompetanser[36]. Det kan være krevende å finne ut hva slags sikkerhetskompetanse virksomheten samlet sett har, og hva som må utvikles eller rekrutteres.

Digdir har sammen med NSM og DFØ samlet de mest aktuelle tilnærmingene til et helhetlig sikkerhetsarbeid, og viser hvordan ulike deler av en virksomhet har ulik forståelse av risiko.

Digdir har også laget en god oversikt over kompetansebeskrivelser [1] i hovedsak med utgangspunkt i arbeidet med informasjonssikkerhet.

3.3 Gjennomfør overordnede risiko- og sårbarhetsanalyser (ROS)

Sikkerhet og beredskap i sin fulle bredde er stort og favner bredt. Styringsaktiviteter og sikringstiltak som skal redusere risiko for intenderte sikkerhetshendelser, vil ikke nødvendigvis redusere risiko for hendelser som har årsak i andre faktorer og forhold, men som likevel truer verdiene.

ROS-analysen[37] 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 virksomhetens verdier. Gjennom å vurdere hva som kan skje, med tilhørende usikkerhet, er det mulig å identifisere og iverksette relevante tiltak som kan bidra til å forhindre at den aktuelle hendelser inntreffer, eller som kan redusere konsekvensene, dersom hendelsen ikke kan unngås. ROS-analysen er et utgangspunkt for utvikling av krise- og beredskapsplaner og planlegging av øvelser.

Bruk Veileder i risiko- og sårbarhetsanalyser for kunnskapssektoren, utviklet av Beredskapsrådet.

3.4 Ta personellsikkerhet og sikkerhetsopplæring på alvor

Ansatte i forskning og utdanning utøver sitt arbeid i et åpent og internasjonalt landskap. Kunnskapsdeling, relasjonsbygging og samarbeid over landegrenser er strategiske målsetninger, og helt nødvendig for å løse utfordringene verdenssamfunnet står ovenfor. Dette representerer også en del sikkerhetsutfordringer. Ansvarlig internasjonalt samarbeid[38] er satt på agendaen for å redusere risikoer som ikke er akseptable.

Spionasje- og innsidetrusselen er til stede i norsk forskning og utdanning. Havet, kysten og våre nordområder har strategisk betydning, og er interessante for fremmed etterretning. Vi er langt fremme innenfor en del kunnskap- og teknologiområder som kan ha militær relevans.

---

[36] Ulike perspektiver gir ulikt fokus | Digdir
[37] Veileder i risiko- og sårbarhetsanalyser for kunnskapssektoren | Universitetet i Stavanger (uis.no)
[38] https://hkdir.no/vaare-tenester/retningslinjer-for-ansvarlig-internasjonalt-samarbeid

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

Eksportkontrollregelverket fordrer derfor søknad og forvaltning av tillatelse til kunnskapsdeling[39] med personer fra enkelte nasjoner, innenfor noen av disse sensitive fagområdene.

En god forståelse av eget risikobilde gjør at virksomheter kan identifisere personellsikkerhetsmessige tiltak som begrenser trussel aktørenes mulighetsrom og som øker virksomhetens egen sikkerhetsmessige robusthet. Tiltak innenfor personellsikkerhet utgjør derfor en viktig del av virksomhetens arbeid for å beskytte verdiene sine.

En forutsetning for forebyggende sikkerhetsarbeid og hensiktsmessig handtering av kritiske situasjoner, er den enkeltes personlige handlingskompetanse. At hver medarbeider og student vet hva de selv kan gjøre i ulike situasjoner og hvor de kan få hjelp. Opplæring og tilgang til relevant sikkerhetsinformasjon er derfor avgjørende. Det bidrar både til å redusere risiko og tilfredsstille lovkrav.

Sikresiden.no er laget av og for UH-sektoren for å gir studenter og ansatte en felles inngang til hva de selv kan gjøre for å bidra i det forebyggende sikkerhetsarbeidet og hva de kan gjøre når noe skjer. Informasjonen er lett å finne og enkel å bruke i konkrete situasjoner.

Ledere har et overordnet ansvar for å påse at virksomheten har tilstrekkelig med kompetanse og ressurser til å ivareta en god personellsikkerhet. Det er ledernes ansvar å sikre at sikkerhetskulturen er sterk, at sårbarheter fanges opp, og at sikkerhetsrelaterte hendelser håndteres effektivt.

For å gi virksomheter et utgangspunkt i arbeidet med personellsikkerhet, har NSM utarbeidet grunnprinsipper for personellsikkerhet[40]. Grunnprinsippene beskriver hva virksomhetene bør gjøre, hvorfor det bør gjøres, men i liten grad hvordan det bør gjøres. Valg av konkrete personellmessige tiltak bør som alltid baseres på virksomhetens egne behov, muligheter, krav og begrensinger.

Få personellsikkerhet og sikkerhetsopplæring inn i styringssystemet for sikkerhet.

Gi ansatte og studenter handlingskompetanse innenfor relevante sikkerhetsområder.

Bruk ressursene i www.sikresiden.no i arbeidet med opplæring og sikkerhetskultur.

---

[39] Retningslinjer for kontroll med kunnskapsoverføring - regjeringen.no
[40] Introduksjon - Nasjonal sikkerhetsmyndighet (nsm.no)

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