**Styringsdokument for sikkerhet og beredskap**

**ved OsloMet**

|  |  |
| --- | --- |
| Type dokument | Styringsdokument |
| Forvaltes av | OI-direktør |
| Godkjent av | Rektor |
| Klassifisering | Åpent |
| Gjelder fra | 16.08.2024 |
| Gjelder til | Neste revisjon |
| Unntatt offentlighet | Nei |
| Referanse rammeverk | NSMs grunnprinsipper for sikkerhetsstyring[[1]](#footnote-2) |
| Referanse Lovverk og føringer | Sikkerhetsloven og virksomhetssikkerhetsforskriften,  Styringsdokument for arbeid med sikkerhet og beredskap i Kunnskapsdepartementets sektor. |
| Referanse interne dokumenter | Underliggende policyer, retningslinjer og prosedyrer. |
| Versjon | 1.0 (Ny) |

Innhold

[Styringsdokument for sikkerhet og beredskap 3](#_Toc166066429)

[1. Prinsipper for sikkerhetsstyring 3](#_Toc166066430)

[1.1 Identifisere og kartlegge 3](#_Toc166066431)

[1.2 Beskytte og opprettholde 3](#_Toc166066432)

[1.3 Oppdage 3](#_Toc166066433)

[1.4 Håndtere og gjenopprette 3](#_Toc166066434)

[1.5 Akseptabel risiko 4](#_Toc166066435)

[2. Sikkerhetsmål 4](#_Toc166066436)

[3. Sikkerhetsstrategi 5](#_Toc166066437)

[3.1 Sikkerhetsstyring er virksomhetsstyring 5](#_Toc166066438)

[3.2 Sikkerhet er et lederansvar 5](#_Toc166066440)

[3.3 Sikkerhetsorganisasjonen tilrettelegger og er pådrivere i sikkerhetsarbeidet 5](#_Toc166066441)

[3.4 Opplæring og sikkerhetskompetanse får styringssystemet til å virke 5](#_Toc166066442)

[4 Styringssystem for sikkerhet og beredskap 6](#_Toc166066443)

[4.1 Sikkerhetsområder 6](#_Toc166066444)

[4.1.1 Beredskap og kontinuitet 6](#_Toc166066445)

[4.1.2 Brannvern 6](#_Toc166066446)

[4.1.3 Fysisk sikkerhet 6](#_Toc166066447)

[4.1.4 Helse, miljø- og sikkerhet (HMS) 6](#_Toc166066448)

[4.1.5 Informasjonssikkerhet og personvern 6](#_Toc166066449)

[4.1.6 Personellsikkerhet 7](#_Toc166066450)

[4.1.7 Kontroll med kunnskapsoverføring (Eksportkontroll og Sanksjoner) 7](#_Toc166066451)

[4.1.8 Nasjonal sikkerhet (Sikkerhetsloven og behandling av gradert informasjon) 7](#_Toc166066452)

[4.2 Styringssystemets dokumentstruktur og forvaltning 7](#_Toc166066453)

[4.2.1 Styrende del 7](#_Toc166066454)

[4.2.2 Gjennomførende del 7](#_Toc166066455)

[4.2.3 Kontrollerende del 7](#_Toc166066456)

[5 Roller og ansvar i styringssystem for sikkerhet og beredskap 8](#_Toc166066457)

[5.1 Linjeorganisasjonen 9](#_Toc166066458)

[5.2 Sikkerhetsorganisasjonen 10](#_Toc166066459)

[5.3 Beredskapsorganisasjonen 13](#_Toc166066460)

# Styringsdokument for sikkerhet og beredskap

OsloMet sine verdier er menneskers liv og helse, informasjon og informasjonssystemer, materiell og objekter. Dette styringsdokumentet angir overordnede prinsipper, sikkerhetsmål og strategier for det systematiske arbeidet som skal beskytte OsloMet sine verdier.

Styringsdokumentet samler og setter rammene for hva som inngår i OsloMet sitt helhetlige styringssystem for sikkerhet og beredskap. Styringsdokumentet beskriver roller og ansvar i styringssystemet, og hvordan dette er fordelt i linjeorganisasjonen, sikkerhetsorganisasjonen og beredskapsorganisasjonen. Styringsdokumentet skal revideres minimum årlig eller ved behov.

# Prinsipper for sikkerhetsstyring

OsloMet sine vedtatte prinsipper for virksomhetsstyring gjelder også for sikkerhetsstyringen. Som overordnede faglige prinsipper for sikkerhets- og beredskapsarbeidet, skal Nasjonal Sikkerhetsmyndighet (NSM) sine 4 grunnprinsipper for sikkerhetsstyring legges til grunn[[2]](#footnote-3):

## 1.1 Identifisere og kartlegge

OsloMet skal ha oversikt over interne og eksterne krav, egne verdier, farer og trusler sårbarheter og avhengigheter, og utarbeide scenarier for uønskede hendelser med konsekvensvurderinger.

## 1.2 Beskytte og opprettholde

Sikkerhetstiltak skal baseres på risikovurderinger, slik at risikoen reduseres til et akseptabelt nivå. Akseptabel sikkerhet oppnås når både organisatoriske, digitale, fysiske, og menneskelige tiltak er kombinert og virker sammen i et helhetlig forebyggende sikkerhetsarbeid.

## 1.3 Oppdage

Sikkerhetsarbeidet skal periodisk kontrolleres for å avdekke om verdiene er forsvarlig sikret iht. akseptabel risiko. Basert på ledelsens gjennomgang skal ledelsen vurdere om sikkerhetsarbeidet er hensiktsmessig, og om det er behov for endringer.

1.4 Håndtere og gjenopprette

Uønskede hendelser skal håndteres for å begrense skade, sikre kontinuitet, gjenopprette, og hindre gjentagelse. Håndtering av uønskede hendelser inngår i det forebyggende sikkerhetsarbeidet.

## 1.5 Akseptabel risiko

Sikkerhetsstyring handler om å håndtere risiko, avdekket gjennom risikovurderinger. Etter risikovurdering skal det vurderes hvordan risiko kan håndteres for å bli akseptabel.

Risiko kan håndteres på ulike måter:

* Unngås, ved å ikke å gjennomføre aktivitet som representerer risiko
* Overføres, ved å flytte en del av ansvaret for risikohåndteringen
* Reduseres, ved å gjennomføre tiltak slik at restrisikoen blir akseptabel
* Akseptere risiko slik den foreligger

Hva som er akseptabel risiko, skal følge av gjeldene akseptkriterier for risikostyring, og gjeldende konsekvensmatriser ved OsloMet.

# Sikkerhetsmål

​

* 1. Helhetlig sikkerhetsstyring skal understøtte OsloMet sitt samfunnsoppdrag, kjernevirksomhet, tillit og omdømme. Sikkerhetsarbeidet skal bidra til gjennomføring av strategier, arbeidet med kvalitet, og andre satsninger. Behovet for sikkerhet skal balanseres med behovet for åpenhet og internasjonalt samarbeid. OsloMet sine campuser skal være trygge arbeids- og studiesteder.
  2. Verdiene skal være tilstrekkelig sikret mot misbruk, skade og tap, basert på en begrunnet og akseptert risiko, og etterlevelse av regulatoriske krav og føringer.
  3. Et helhetlig og systematisk forebyggende sikkerhetsarbeid skal gjøre OsloMet robust og godt forberedt for å kunne holde driften i gang og redusere skade og konsekvenser av alvorlige og langvarige hendelser.
  4. Ansatte, studenter og tilknyttede skal ha tilstrekkelig sikkerhetskompetanse for å kunne bidra til forebyggende sikkerhet i sitt daglige virke. De skal vite hva de skal gjøre og hvor de skal si fra ved uønskede hendelser.

# Sikkerhetsstrategi

For å nå sikkerhetsmålene, skal arbeidet med sikkerhet være risikobasert, systematisk, helhetlig på tvers av sikkerhetsområder, og inngå som en del av virksomhetsstyringen. Opplæringsressursene fra sikresiden.no skal brukes systematisk.

## 3.1 Sikkerhetsstyring er virksomhetsstyring

## Øverste ledelse skal årlig få en oversikt over risiko, måloppnåelse og etterlevelse av krav samt forslag til tiltak for å redusere risiko. Dette skal behandles i ledelsens gjennomgang.

1. Øverste ledelse skal ha kunnskapsgrunnlag for beslutninger i plan- og budsjettprosessen for å redusere risikoen til et akseptabelt nivå.
2. Styret skal ha tilstrekkelig informasjon til å ivareta sin påse-rolle.

## Sikkerhet er et lederansvar

1. Enhver leder skal være kjent med styringssystemet, og innenfor sitt ansvars- og myndighetsområde kunne rapportere på:
2. Vurderinger av egne verdier, trusler og sårbarheter.
3. Gjennomføring av risikovurderinger, som følges opp med tiltak for å redusere risikoen til et akseptabelt nivå.
4. Sikkerhetsopplæring og sikkerhetsoppfølging av egne ansatte og tilknyttede.

## Sikkerhetsorganisasjonen tilrettelegger og er pådrivere i sikkerhetsarbeidet

1. Sikkerhetsorganisasjonen skal koordinere arbeidet med en årsplan som det rapporteres på i linjen og i sikkerhetsorganisasjonen.
2. Sikkerhetstiltak skal være basert på risiko og fungere godt sammen.
3. Etablerte rammeverk, grunnprinsipper og anerkjente veiledninger skal brukes for å utvikle og følge god praksis.
4. Sikkerhetsarbeidet skal kontinuerlig forbedres og tilpasses aktuelt risikobilde.

## Opplæring og sikkerhetskompetanse får styringssystemet til å virke

1. Alle skal ha jevnlig basisopplæring i sikkerhet.
2. Det skal vurderes hvilken sikkerhetsopplæring ulike ansatte, studenter og tilknyttede trenger i tillegg til basisopplæringen.
3. Sikresiden.no skal være synlig og lett å finne for OsloMet sine ansatte, studenter og tilknyttede. Sikresiden.no skal være synlig i lokalene og opplæringsressursene fra sikresiden.no skal brukes inn i virksomhetsprosesser der de hører hjemme.
4. Alle med roller i beredskapsstabene skal ha jevnlige øvelser for å sikre operativ handlingskompetanse og effektiv bruk av beredskapsplanverk og verktøy for samhandling og proaktiv stabsmetodikk.

# Styringssystem for sikkerhet og beredskap

Styringssystem for sikkerhet og beredskap samler og setter rammene for helhetlig sikkerhetsstyring på tvers av sikkerhetsområder, deres regulatoriske krav og deres risikobilde.

## 4.1 Sikkerhetsområder

De ulike sikkerhetsområdene har ulikt hovedfokus, samtidig som de henger sammen og er delvis avhengige av hverandre.

### 4.1.1 Beredskap og kontinuitet

Beredskap er definert som planlagte og forberedte tiltak som gjør oss i stand til å håndtere uønskede hendelser slik at konsekvensene blir minst mulig[[3]](#footnote-4). Kontinuitet handler om å kunne opprettholde aktivitet til tross for en uønsket hendelse, og å sørge for at verdiskapingen i et system, en tjeneste eller en arbeidsprosess kan holdes i gang[[4]](#footnote-5).

### 4.1.2 Brannvern

Arbeidet med brannvern skal bidra til å redusere sannsynligheten for brann, og begrense konsekvensene som brann kan få for liv, helse, miljø og materielle verdier[[5]](#footnote-6), og for drift.

### 4.1.3 Fysisk sikkerhet

Fysisk sikkerhet er tiltak som beskytter verdier mot at noen får urettmessig tilgang. Styrken i tiltakene varierer med verdivurderingen av det som skal sikres. Fysiske sikringstiltak er helt grunnleggende uavhengig av type trussel og virksomhet[[6]](#footnote-7).

### 4.1.4 Helse, miljø- og sikkerhet (HMS)

Et systematisk HMS-arbeid skal fremme at virksomheten har et forbedringsarbeid innen arbeidsmiljø, sikkerhet, forebygging av helseskader eller miljøforstyrrelser, vern av ytre miljø, forebygging av uhell og ulykker forbundet med egen lovlig aktivitet, og forebygging av uønskede tilsiktede hendelser[[7]](#footnote-8).

### 4.1.5 Informasjonssikkerhet og personvern

Informasjonssikkerhet handler om å sikre informasjonsbehandling, som foregår i samspill mellom mennesker, prosesser og teknologi. Personvern er individets rett til privatliv og kontroll over egne personopplysninger. Kunnskapsdepartementet har fastsatt *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning*, som beskriver krav til forsvarlig informasjonsbehandling, IT-sikkerhet og personvern[[8]](#footnote-9).

### 4.1.6 Personellsikkerhet

Personellsikkerhet handler om å gjennomføre tiltak som gjør at mennesker bidrar til god sikkerhet gjennom sine holdninger, atferd og kultur. Tiltak innenfor personellsikkerhet har særlig fokus på å redusere risiko for bevisst og ubevisst innsidevirksomhet[[9]](#footnote-10).

### 4.1.7 Kontroll med kunnskapsoverføring (Eksportkontroll og Sanksjoner)

Kontroll med kunnskapsoverføring handler om å ikke dele sensitiv kunnskap og flerbruksteknologi med land vi ikke har sikkerhetspolitisk samarbeid med, uten tillatelse. Utenriksdepartementet har utarbeidet retningslinjer for utdanningsinstitusjonene for å ivareta at kunnskapsdeling skjer innenfor rammene av det norske eksportkontrollregelverket og gjeldende sanksjonsforskrifter[[10]](#footnote-11).

### 4.1.8 Nasjonal sikkerhet (Sikkerhetsloven og behandling av gradert informasjon)

Sikkerhetsloven handler om å beskytte verdier med betydning for nasjonale sikkerhetsinteresser. Sikkerhetsloven stiller krav om et dokumentert og virksomhetstilpasset styringssystem som også omfatter aktiviteter som ivaretar nasjonale sikkerhetsinteresser[[11]](#footnote-12).

## 4.2 Styringssystemets dokumentstruktur og forvaltning

Hvert sikkerhetsområde har en dokumentstruktur underlagt dette styringsdokumentet, som skal være tilgengelige for ansatte, studenter og tilknyttede:

### 4.2.1 Styrende del

Policy som angir krav og føringer, prinsipper, mål og strategier, og roller og ansvar for gjennomføring. Policy er overordnet og normativ, og skal godkjennes av Direktør for organisasjon og infrastruktur. Policy skal revideres minimum årlig og endres ved behov.

### 4.2.2 Gjennomførende del

Retningslinjer, prosedyrer/rutiner som beskriver hvordan arbeid med sikkerhet og beredskap skal gjennomføres. Retningslinjer, prosedyrer/rutiner skal godkjennes av sikkerhetsleder. Gjennomførende del skal revideres minimum årlig og endres ved behov.

### 4.2.3 Kontrollerende del

Dokumentasjon på risikostyring, gjennomførte opplæringsaktiviteter og øvelser, avvik- og hendelseshåndtering, internkontroll, revisjoner, og ledelsens gjennomgang.

# Roller og ansvar i styringssystem for sikkerhet og beredskap

Styringsprosessene ved OsloMet involverer hele organisasjonen, iht. vedtatte styringslinjer.

Dette er også gjeldende for roller og ansvar i styringssystem for sikkerhet og beredskap.

**Styret**

Skal påse at sikkerhet og beredskap inngår i OsloMet sin virksomhetsstyring, i et helhetlig styringssystem for sikkerhet. Styret skal orienteres årlig om sikkerhetstilstanden gjennom årsrapporteringen.

**Linjeorganisasjonen**

Rektor er øverste ansvarlige for sikkerheten ved OsloMet. Det strategiske ansvaret er delegert til Direktør organisasjon og infrastruktur.

Enkelte ledere har nøkkelroller i sikkerhetsorganisasjonen i sin administrative enhet. Disse lederne er ansvarlig for at det er kompetanse, ressurser og planer i egen avdeling til å ivareta sikkerhetsområder som faglig tilhører deres ansvars- og myndighetsområde.

Alle ledere er ansvarlige for at styringssystemet gjøres gjeldende i eget ansvars- og myndighetsområde, og for å gjennomføre aktiviteter iht. vedtatte sikkerhetsstrategi, og de til enhver tid gjeldende tiltaks- og handlingsplaner.

**Sikkerhetsorganisasjonen**

Sikkerhetsorganisasjonen bistår både i styrende, gjennomførende og kontrollerende del i styringssystemet. Sikkerhetsorganisasjonen består av sikkerhetsleder (CSO), informasjonssikkerhetsleder (CISO), og andre nøkkelroller for de ulike sikkerhetsområdene.

**Beredskapsorganisasjonen**

Beredskapsorganisasjonen består av roller som inngår i OsloMet sine beredskapsstaber sentralt og på fakultet, som beskrevet i OsloMet sin beredskapsplan.

**Alle**

Alle ansatte, studenter og tilknyttede har et selvstendig ansvar for å ivareta sikkerheten i egne aktiviteter, og for å si fra dersom de oppdager feil, uhell eller sikkerhetstruende hendelser. Alle skal delta i opplæring og bidra til at OsloMet har en god sikkerhetskultur.

**Internrevisjonen**

Har en uavhengig kontrollrolle. Internrevisjonen gjennomfører revisjon av OsloMet sin sikkerhetsstyring, innenfor hele eller deler av styrende, gjennomførende og kontrollerende del.

## 5.1 Linjeorganisasjonen

**Rektor**

* Er øverste ansvarlig for at sikkerhetsstyringen ved OsloMet inngår som del av øvrige plan- og styringsprosesser.
* Er behandlingsansvarlig for personopplysninger, og autorisasjonsansvarlig iht. sikkerhetslovens bestemmelser. Rektor orienterer årlig Styret om sikkerhetsarbeidet.
* Godkjenner styringsdokument for sikkerhet og beredskap.

**Prorektorer, dekaner, instituttledere, instituttdirektører, senterleder og alle ledere i linjen**

* Alle ledere er ansvarlige for at styringssystemet gjøres gjeldende og relevant i eget ansvars- og myndighetsområde.
* Alle ledere skal gjennomføre aktiviteter iht. vedtatte sikkerhetsstrategi og de til enhver tid gjeldende tiltaks- og handlingsplaner.

**Direktør Organisasjon og infrastruktur**

* Er strategisk ansvarlig for at styringssystemet holdes oppdatert, kommunisert og relevant, og for at sikkerhetsorganisasjonen har riktig ressurser, økonomi og kompetanse.
* Godkjenner styrende del (policy) i alle sikkerhetsområdene.
* Er ansvarlig for at sikkerhetsorganisasjonen utvikler tjenester, prosesser og funksjoner som bistår linjeorganisasjonen i å gjennomføre av sikkerhetskravene.
* Har nøkkelrollene sikkerhetsleder (CSO), informasjonssikkerhetsleder (CISO), Fagansvarlig personvern, og Fagansvarlig beredskap og kontinuitet i sin administrative enhet.

**Prorektor forskning**

* Er ansvarlig for at det er kompetanse, ressurser og planer i eget ansvars- og myndighetsområde for å ivareta arbeidet med kontroll med kunnskapsoverføring (eksportkontroll og sanksjoner).
* Har nøkkelrollen Fagansvarlig kunnskapsoverføring som strategisk og gjennomførende støtte, i samarbeid med den øvrige sikkerhetsorganisasjonen.

**Avdelingsdirektør IT**

* Har nøkkelrollene IT-sikkerhetsleder og Computer Security Incident Response Team (CSIRT) i sin administrative enhet.
* Er ansvarlig for at det er kompetanse, ressurser og planer i egen avdeling til å ivareta IT-sikkerheten og personvernet i tråd med gjeldende krav.
* Er ansvarlig for at informasjonssikkerheten og personvernet ivaretas i OsloMet sin IT-infrastruktur, systemer og tjenester.

**Avdelingsdirektør Eiendom**

* Har nøkkelrollene Fagansvarlig brannvern og Fagansvarlig fysisk sikkerhet i sin administrative enhet.
* Er ansvarlig for at det er kompetanse, ressurser og planer i egen avdeling til å ivareta fagansvaret for brannvern og fysisk sikkerhet.
* Er ansvarlig for at brannvern og fysisk sikkerhet ivaretas ved OsloMet.

**Avdelingsdirektør HR**

* Har nøkkelrollene Fagansvarlig personellsikkerhet og Fagansvarlig HMS i sin administrative enhet.
* Er ansvarlig for at det er kompetanse, ressurser og planer i egen avdeling til å ivareta fagansvaret for Helse, - Miljø- og Sikkerhet (HMS-system) og for Personellsikkerhet.

## 5.2 Sikkerhetsorganisasjonen

Sikkerhetsorganisasjonen består av nøkkelroller som har både strategiske og operative oppgaver:

* Utarbeider policyer, retningslinjer og prosedyrer/rutiner, med planer for oppfølging
* Koordinerer, tilrettelegger og er pådrivere for arbeidet innen de ulike sikkerhetsområdene
* Gir opplæring og veiledning i sikkerhetsfaglige spørsmål og bistår med gjennomføring av forebyggende aktiviteter
* Bistår med å håndtere avvik- og sikkerhetshendelser

De som innehar rollene i sikkerhetsorganisasjonen skal møtes jevnlig, for å ivareta tverrfaglig samarbeid og situasjonsforståelse, og for å utarbeide og gjennomføre koordinerte planer og aktiviteter.

Enkelte nøkkelroller har ansvar for å koordinere sikkerhetsfaglige nettverk og forum, for å sikre samhandling med operative ressurser i organisasjonen.

Rollene i sikkerhetsorganisasjonen har egne rollekort, og skal rapportere til egen leder, til OI-direktør, til sikkerhetsleder, og til øvrige i sikkerhetsorganisasjonen etter gjeldende HUKI-matrise[[12]](#footnote-13).

**Sikkerhetsleder (CSO)**

* Koordinerer sikkerhetsarbeidet på tvers av alle sikkerhetsområdene.
* Ansvarlig for at sikkerhetsorganisasjonen videreutvikler policy, retningslinjer og prosedyrer/rutiner innenfor alle sikkerhetsområder.
* Godkjenner gjennomførende del (retningslinjer, rutiner/prosedyrer) i alle sikkerhetsområdene.
* Utvikler og følger opp policy, retningslinjer og rutiner/prosedyrer for *nasjonal sikkerhet (behandling av gradert informasjon)*
* Legger frem årlig ledelsens gjennomgang for den helhetlige sikkerhetsstyringen

**Informasjonssikkerhetsleder (CISO)**

* Utvikler og følger opp policy, retningslinjer og prosedyrer/rutiner i *ledelsessystem for informasjonssikkerhet og personvern*.
* Koordinerer informasjonssikkerhetsarbeidet og holder oversikt over informasjonssikkerhetsrisiko, måloppnåelse og etterlevelse av krav.

**IT-sikkerhetsleder**

* Utvikler og følger opp retningslinjer og prosedyrer/rutiner for IT-sikkerhet, i *ledelsessystem for informasjonssikkerhet og personvern.*
* Leder arbeidet med sikkerhetsarkitektur, teknisk sikring av IKT-systemene, sårbarhetsscanning og overvåkning av sikker tilstand i IKT-systemene.

**Computer Security Incident Response Team (CSIRT)**

* Detekterer og håndterer cyberangrep.
* Samvirker med Cybersikkerhetssenter for forskning og utdanning (eduCSC) og Norsk cybersikkerhetssenter (NCSC).

**Fagansvarlig Personvern**

* Utvikler og følger opp retningslinjer og prosedyrer/rutiner for personvern, og kravene til personvern i *ledelsessystem for informasjonssikkerhet og personvern.*
* Koordinerer arbeidet med etterlevelse av personvernregelverket, leder nettverk for personvernkontakter, og følger opp avvikshåndtering og oppmelding til Datatilsynet.

**Fagansvarlig Kunnskapsoverføring (eksportkontroll og sanksjoner)**

* Utvikler og følger opp Policy, retningslinjer og prosedyrer/rutiner for Kontroll med kunnskapsoverføring (eksportkontroll og sanksjoner)
* Er rådgiver og saksbehandler ved søknad om lisens for kunnskapsoverføring.

**Fagansvarlig Personellsikkerhet**

* Utvikler og følger opp policy, retningslinjer og prosedyrer/rutiner for personellsikkerhet.
* Koordinerer arbeidet med sårbarhetsoppfølging og innsiderisiko, og med systematisk sikkerhetsopplæring innenfor alle sikkerhetsområdene, med bl.a. bruk av Sikresiden.no.

**Fagansvarlig HMS**

* Utvikler og følger opp policy, retningslinjer og prosedyrer/rutiner for HMS.
* Koordinerer arbeidet med HMS, og leder nettverk for HMS-kontakter.

**Fagansvarlig Brannvern**

* Utvikler og følger opp policy, retningslinjer og prosedyrer/rutiner for brannvern.
* Koordinerer arbeidet med brannvern, og får tiltak gjennomført.

**Fagansvarlig Fysisk sikkerhet**

* Utvikler og følger opp policy, retningslinjer og prosedyrer/rutiner for fysisk sikkerhet.
* Koordinerer arbeidet med fysisk sikkerhet, og får tiltak gjennomført.

**Fagansvarlig Beredskap og kontinuitet**

* Utvikler og følger opp policy, retningslinjer og prosedyrer/rutiner for beredskap og kontinuitet.
* Utvikler, vedlikeholder og tilgjengeliggjør beredskapsplanverket, og gjennomfører og følger opp beredskapsøvelser.

**Personvernombud (Personvernombudstjeneste fra Sikt)[[13]](#footnote-14)**

* Er en uavhengig stilling og skal støtte OsloMet i å oppfylle pliktene etter personvernregelverket, ved å gi uavhengige råd til ledelse og ansatte, og ved å kontrollere etterlevelse.
* Skal være kontaktpunkt for de registrerte og samarbeide med Datatilsynet.

## 5.3 Beredskapsorganisasjonen

Beredskapsorganisasjonen skal bygges etter de nasjonale beredskapsprinsippene[[14]](#footnote-15), som stadfester at det daglige linjeansvaret og den daglige sikkerhetsorganisasjonen også gjelder ved kriser:

* **Ansvarsprinsippet** som betyr at den som har et ansvar i en normalsituasjon også har dette ansvaret ved krisehendelser.
* **Likhetsprinsippet** som betyr at den organisasjonen som skal håndtere en krise, er mest mulig lik den daglige organisasjonen.
* **Nærhetsprinsippet** som betyr at kriser skal håndteres på lavest mulig nivå.
* **Samvirkeprinsippet** som betyr at krisehåndteringen skal skje i samvirke med andre berørte aktører og virksomheter, både i det forebyggende arbeidet, og når noe skjer.

Sentral beredskapsledelse, og fakultetenes beredskapsledelse er beskrevet i beredskapsplan.

1. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/introduksjon/> [↑](#footnote-ref-2)
2. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/introduksjon/> [↑](#footnote-ref-3)
3. [Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor - regjeringen.no](https://www.regjeringen.no/no/dokumenter/styringsdokument-for-arbeidet-med-samfunns-sikkerhet-og-beredskap-i-kunnskapssektoren/id2512037/?ch=3) [↑](#footnote-ref-4)
4. [Veileder kontinuitetsplan for informasjonssikkerhetshendelser versjon 1 (sikt.no)](https://cms.sikt.no/sites/default/files/2023-10/Veileder%20kontinuitetsplan%20for%20informasjonssikkerhetshendelser%20versjon%201.pdf) [↑](#footnote-ref-5)
5. <https://lovdata.no/forskrift/2015-12-17-1710/§1> [↑](#footnote-ref-6)
6. [Fysisk sikring - Nasjonal sikkerhetsmyndighet (nsm.no)](https://nsm.no/fysisk/fysisk-sikring/) [↑](#footnote-ref-7)
7. <https://lovdata.no/forskrift/1996-12-06-1127/§1> [↑](#footnote-ref-8)
8. [Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning (regjeringen.no)](https://www.regjeringen.no/contentassets/cfb4f2cc8f744cb2acf6d0df4027df7d/policy-for-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning.pdf) [↑](#footnote-ref-9)
9. [Introduksjon - Nasjonal sikkerhetsmyndighet (nsm.no)](https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/introduksjon/) [↑](#footnote-ref-10)
10. [https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/om-eksportk ontroll/kunnskap/id2500543/](https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/om-eksportk%20ontroll/kunnskap/id2500543/) [↑](#footnote-ref-11)
11. <https://www.regjeringen.no/no/dokumenter/styringsdokument-for-arbeidet-med-samfunns-sikkerhet-og-beredskap-i-kunnskapssektoren/id2512037/?ch=8> [↑](#footnote-ref-12)
12. En modell som benyttes for å definere roller og ansvarsområder. HUKI står for hovedansvarlig, utførende, konsulteres og informeres. [HUKI - PRINCE2 wiki](https://prince2wiki.no/knowledge-base-2/huki/) [↑](#footnote-ref-13)
13. <https://sikt.no/tjenester/personvernombud> [↑](#footnote-ref-14)
14. [Meld. St. 29 (2011–2012) (regjeringen.no)](https://www.regjeringen.no/contentassets/bc5cbb3720b14709a6bda1a175dc0f12/no/pdfs/stm201120120029000dddpdfs.pdf) [↑](#footnote-ref-15)