Veileder til personellsikkerhet i UH-sektoren

Sikkerhet i rekruttering og oppfølging av personell

Tilgang på kunnskap, kompetanse og teknologi blir stadig viktigere i den globale konkurransen om makt og innflytelse, og dermed også for den nasjonale sikkerheten. Dette får implikasjoner for alle aktører i forskningssystemet.

Meld. St. 14 (2024-2025): 46

TIL HØRING 20.04. – 07.05.2026

Veileder til personellsikkerhet i UH-sektoren
Sikresiden.no og HK-dir 2026

Innhold

Om denne veilederen

Denne veilederen er utarbeidet på bakgrunn av et uttrykt ønske fra virksomhetene om en felles tilnærming til personellsikkerhet.

Veilederen er utviklet av Direktoratet for høyere utdanning og kompetanse (HK-dir) og sikresiden.no (Sikresiden). Sikresiden er et samarbeid mellom de fleste virksomheter i norsk UH-sektor som utvikler felles ressurser innen sikkerhet.

Veilederen støtter seg på grunnprinsipper, håndbøker og terminologi for personellsikkerhet utviklet av Nasjonal sikkerhetsmyndighet, og tilpasser disse til UH-virksomhetenes egenart. Veilederen støtter seg også på rapporter, kurs og veiledere fra andre sektorer.

Virksomheter i sikresiden-samarbeidet har bidratt med egne erfaringer og lagt til rette for at deres faktiske problemstillinger blir belyst i veilederen.

Veilederen er primært for dem som

- skal utvikle og tilrettelegge for et helhetlig og systematisk arbeid med personellsikkerhet

Veilederen er også nyttig for alle som

- rekrutterer og følger opp personell
- har roller innen sikkerhetsstyring, forskningssikkerhet og informasjonssikkerhet
- jobber med sikkerhetsopplæring, lederopplæring og sikkerhetskultur
- jobber innen vernelinjen, arbeidsrett og fagforeningene
- jobber med organisasjonsutvikling og psykososialt arbeidsmiljø

Veilederens oppbygging

1. Del 1 foreslår en tilnærming til personellsikkerhet i UH-sektoren som vektlegger betydningen av sektorens samfunnsoppdrag og egenart.
2. Del 2 handler om sikkerhet i rekrutteringsprosessen, der vurderinger av arbeidets innhold og krav til sikkerhetsmessig egnethet står sentralt. Den gir praktisk støtte til hvilke vurderinger som bør gjøres, og hvilke verktøy og metoder som kan brukes.
3. Del 3 handler om hvordan virksomheter kan etablere og videreutvikle et systematisk arbeid med personellsikkerhet, ved å innlemme personellsikkerhet i sikkerhetsstyringen og i HR-prosessene.
4. Del 4 danner grunnlaget for den praktiske støtten som gis i del 2 og 3. Den går gjennom lov- og regelverk, og andre tungtveiende sikkerhetshensyn av betydning for personellsikkerhet.

Felt med grønn bakgrunn:	**Felt med blå bakgrunn:**	**Felt med rød bakgrunn:**
Veilederens forslag til praktisk tilnærming, anbefalinger til fremgangsmåte, oversikter, sjekklister osv.	Fakta, premisser, lover, sitater og budskap fra relevante myndigheter.	Informasjon om hvordan Sikresiden kan være til hjelp i arbeidet og hvilke ressursen Sikresiden utvikler.

Personellsikkerhet hviler på:

- åpenhet og dialog som fremmer tillit og trygghet
- internkommunikasjon som formidler at sikkerhet handler om å beskytte verdier og medarbeidere
- at ledere og forskningsansvarlige har kompetanse og mulighet til å følge opp medarbeiderne i hverdagen
- et helhetlig og balansert sikkerhetsarbeid hvor menneskelige tiltak sees i sammenheng med fysiske og digitale sikkerhetstiltak

Personellsikkerhet i korthet

Personellsikkerhet handler om å håndtere risiko som ansatte, gjesteforskere og annet tilknyttet personell kan representere ved sin tilgang til *verdier* som skal beskyttes av lov og/eller andre sikkerhetsmessige hensyn.

Verdier i denne sammenheng er kunnskap, kompetanse og teknologi som finnes i form av informasjon og informasjonssystemer, og infrastruktur og objekter.

Risiko i denne sammenheng (ofte omtalt som *innsiderisiko*) er kombinasjonen av verdienes betydning, trusselbildet, og verdienes eksponering og sårbarhet for dette trusselbildet gjennom de ansatte og tilknyttede sin tilgang. Risiko i denne sammenheng handler også om hvilke uønskede hendelser de ansatte og tilknyttede kan utsettes for.

Personellsikkerhet i praksis handler om[1]:

1. **Identifisere og kartlegge:** Å identifisere og kartlegge risiko knyttet til stillinger, oppdrag og rekruttering av nye medarbeidere. Dette er vurderinger som krever kunnskap om virksomhetens verdier og ressurser.

2. **Beskytte:** Å innlemme personellsikkerhet i sikkerhetsstyringen for å håndtere risiko. Å etablere rammer og rutiner innenfor personellsikkerhet bidrar til å beskytte både verdiene og medarbeiderne.

3. **Opprettholde og oppdage:** Dette handler om god sikkerhetskultur og å opprettholde god sikkerhet over tid. Det baserer seg på at medarbeiderne blir fulgt opp så lenge de er tilknyttet virksomheten og at arbeidsforholdet avsluttes på en god måte.

4. **Håndtere og gjenopprette:** Å håndtere sikkerhetsrelaterte hendelser som involverer medarbeidere. Det kan være knyttet til bekymringer, uønskede hendelser eller annet som relateres til personellsikkerhetsmessige forhold.

[1] Introduksjon - Nasjonal sikkerhetsmyndighet

DEL 1 PERSONELLSIKKERHET I UH-VIRKSOMHETER

1.1 UH-sektoren i møte med geopolitikk i endring

Systemene for forskning og utvikling på sivil og militær side samordnes i større grad[2], og Regjeringen ønsker eksempelvis at forskning skal utvikle og anvende sensitive teknologier i tråd med norske og europeiske interesser[3]. Dette reflekteres også i forskningsfinansieringen. Virksomheter og fagmiljø som ønsker å delta i slik forskning må derfor være rigget for å kunne inngå i prosjekter med mer tydelige krav til sikkerhet[4].

UH-sektoren er underlagt sikkerhetsloven

Sikkerhetsloven gjelder for statlige, fylkeskommunale og kommunale organer. Alle KDs underliggende virksomheter er derfor direkte underlagt sikkerhetsloven. Alle virksomheter som omfattes av sikkerhetsloven skal ha et dokumentert styringssystem for sikkerhet. Kravet gjelder uavhengig av om virksomheten har skjermingsverdige verdier. *Regjeringen.no*

De åpne trussel- og risikovurderingene fra norske sikkerhetsmyndigheter understreker at UH-sektoren i økende grad er et mål for fremmed etterretning, uønsket kunnskap- og teknologioverføring, påvirkning og innblanding. Etterretning foregår langsiktig, indirekte og skjult under dekke av noe annet, i et hybrid trusselbilde. UH-virksomhetene kan være en inngangsport til strategisk viktig teknologi og kompetanse, til databaser og registre om befolkningen, og til informasjon innen mange ulike områder. De kan også være en inngang til samfunnskritiske funksjoner og tjenester, til beslutningstakere, offentlige organer og til næringslivet.

[2] Meld. St. 14 (2024–2025) - regjeringen.no
[3] https://www.forskningsradet.no/contentassets/7bd23b01e42146acbb23d256113a2246/kvast-sluttrapport-delleveramne-5-og-6.pdf
[4] https://www.forskningsradet.no/forskningspolitikk-strategi/forskningssikkerhet/

UH-sektoren omtales gjerne som en *godtepose* for fremmed etterretning og andre trusselaktører. Åpenheten, delingen av resultater og innovasjoner og store kontaktflater og internasjonale nettverk kan gjøre sektoren enkel å utnytte.

I dette landskapet må medarbeidere bli mer motstandsdyktige mot å bli manipulert og utnyttet, og verdier og forskning må beskyttes fra å bli misbrukt, skadet eller gå tapt.

Forskerhverdagen er preget av unike sårbarheter som kan bli utnyttet, f.eks.:

- akademisk frihet og stor grad av autonomi
- sterk faginteresse
- internasjonale miljø med formelle og uformelle samarbeidskonstellasjoner
- høye ambisjoner og ønske om anerkjennelse
- hard konkurranse om prosjekter og midler
- uklare fremtidsutsikter

Alle bør ha et reflektert forhold til

- verdien av egen fagkunnskap, sitt personlige nettverk, og tilganger til informasjon, utstyr og lokaler
- hvordan trusselbildet er relevant for eget fagområde og forskningsprosjekt
- hvilke sårbarheter som kan utnyttes
- hvem de samarbeider med
- mulige forskningsetiske dilemmaer
- hvilken risiko som kan foreligge, og hvordan denne kan håndteres

1.2 Så åpen som mulig så sikker som nødvendig

Mer sikkerhet innebærer en balansegang som må ivareta mange hensyn.

Kunnskapssektoren får en stadig viktigere rolle i totalforsvaret, men må balansere nye krav med behovet for å bevare akademisk frihet og sektorens samfunnsoppdrag.

Sissel Jore, leder Beredskapsrådet i kunnskapssektoren, webinar 20.02.2026

UH-sektoren skal hegne om de demokratiske samfunnsverdiene og bidra til nytte for samfunnet. Sikkerhetshensyn må balanseres opp mot forskningsetiske normer[5]:

- **Sannhetsnormen** er ufravikelig i all vitenskapelig virksomhet. Sannhetssøken, sannhetsforpliktelse, redelighet og ærlighet er en forutsetning for forskningens kvalitet og pålitelighet. Sannhetsnormen er knyttet til overordnede metodologiske normer, som saklighet, klarhet, etterrettelighet og etterprøvbarhet.
- **Forskningens integritet** skal sikres ved at forskningen skal være åpen, kollektiv, uavhengig og kritisk (kjent som «vitenskapens etos»). Disse normene konstituerer og regulerer god vitenskapelig praksis og skal sikre forskningens integritet.
- **Forskningens forsvarlighet** handler om menneskeverdet, som blir ivaretatt gjennom tre prinsipper: respekt for likeverd, frihet og selvbestemmelse, beskyttelse mot risiko for skade og urimelig belastning, og rettferdighet i prosedyrer og fordeling av goder og byrder.

En åpen og internasjonalt orientert forskningssektor er viktig for å sikre Norge tilgang på kunnskap, kompetanse og teknologi, styrke norsk konkurransekraft og bidra til å finne løsninger på globale utfordringer. *Meld. St. 14 (2024-2025), s.68*

Personellsikkerhet er viktig for forskningssikkerheten

Forskningssikkerhet er nøkkelen til fortsatt internasjonalt samarbeid, og er identifiseringen og håndteringen av risiko knyttet til

1. uønsket kunnskaps- og teknologioverføring
2. uønsket påvirkning og innblanding samt
3. brudd på forskningsetikk og faglig integritet gjennom bruk av kunnskap og teknologi til å underminere sentrale samfunnsverdier.

Meld. St. 14 (2024-2025): 48[11] (som gjengir EUs definisjon)

Håndtering av risiko må også ivareta viktige lovpålagte hensyn, som:

[5] Introduksjon til forskningsetikk | Forskningsetikk

- **Akademisk frihet:** Universitets- og høgskoleloven lovfester ansvaret for å fremme og verne akademisk frihet og beskytte dem som utøver den. Loven påpeker at virksomhetene skal samarbeide med relevante aktører både nasjonalt og internasjonalt.
- **Kvalifikasjonsprinsippet:** Statsansatteloven krever at kvalifikasjonsprinsippet overholdes, med mindre det det er unntak i lov eller forskrift.
- **Arbeidsgiveransvaret:** Arbeidsmiljøloven pålegger arbeidsgiver en omsorgsplikt, og skal ivareta grunnleggende rettigheter som rettferdige arbeidsforhold. Den enkeltes integritet, verdighet og grunnleggende rettigheter skal ivaretas.
- **Personvernet:** Personopplysingsloven lovfester ansvaret om å beskytte enkeltpersonens personopplysninger, og sikre at disse behandles ut fra et lovmessig forankret grunnlag på en rettferdig og transparent måte.
- **Diskrimineringsvernet:** Likestillings- og diskrimineringsloven gir vern mot å bli diskriminert. En eventuell forskjellsbehandling må være godt og saklig dokumentert.

Kunnskap, kompetanse og forskning er blitt helt sentrale ressurser i et mer sammensatt og hybrid trusselpreget sikkerhetslandskap. Akademia kan derfor ikke kun være en «tilskuer», men er en kompetanseaktør i nasjonal sikkerhet.

Sissel Jore, leder Beredskapsrådet i kunnskapssektoren, webinar 20.02.2026

1.3 Bevisstgjøring og opplæring er kjernen i personellsikkerhet

Ledere og medarbeidere må ha mulighet, vilje og evne til å vurdere og håndtere risiko i arbeidshverdagen. Verdier, trusler og sårbarheter må gjøres snakkbart og håndterlig. Personellsikkerhet handler derfor i stor grad om systematisk bevisstgjøring og opplæring.

Dette bør forankres i rutiner, og gjennomføres naturlig i prosesser der det hører hjemme.

Bevisstgjøring og opplæring bør inn

- i introduksjonsprogram for nye medarbeidere
- som et fast tema i medarbeidersamtaler
- ved endringer i arbeidsoppgaver

- før aktivitet med forhøyet risiko, som reiser til risikoland, konferanser og arrangementer innen sensitive eller kontroversielle fagområder, eller ved delegasjonsbesøk
- for dem som jobber i spesielt trusselutsatte fagmiljøer, på laboratorier eller med store eller sensitive datasett
- for ansatte med omfattende systemtilganger

1.4 Ledere må ha kompetanse

Sikkerhetsmessig ledelse starter på øverste ledernivå, og følger hele leder- og ansvarslinjen. I tillegg til lederlinjen, har UH-sektoren ulike lederroller uten formelt personalansvar, som i mange tilfeller de nærmeste til å følge opp forskerne.

Lederansvaret innebærer å gi nødvendige rammebetingelser for sikkerhets- og beredskapsarbeidet. Det innebærer også ansvaret for å motivere medarbeidere til å handle på måter som ivaretar sikkerhet og beredskap. Medarbeidere må vite hva som forventes av dem og forstå hvorfor sikkerhetstiltakene eksisterer.

Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor (s. 13)

For mange ledere kan det oppleves nytt og uvant at sikkerhet også skal inngå i oppfølgningen av medarbeiderne. NSM kaller dette *sikkerhetsmessig ledelse* og understreker at det i stor grad handler om å kjenne sine medarbeidere. Derfor er det viktig at ledere snakker med sine medarbeidere om sikkerhet.

Hva må ledere kunne gjøre?

Ledere har ansvar for å håndtere risiko i egen enhet. De har også ansvar for at arbeidsmiljøet inngir trygghet, tillit, åpenhet og dialog.

- Ledere bør ha innsikt i verdiene som forvaltes i enheten, hva som truer dem, og hvilke sårbarheter som kan utnyttes.
- Ledere bør legge til rette for refleksjon og diskusjon om verdier, trusler og sårbarheter, for eksempel i form av hendelser, scenarier og dilemmaer som er relevante for medarbeidernes hverdag. Dette vil gjøre det lettere å identifisere og

håndtere relevante problemstillinger og man etablerer et felles språk for å snakke om dette.

- Ledere må ha evne og vilje til å gjennomføre forebyggende samtaler om sikkerhet, og oppfølgingssamtaler ved behov.
- Ledere har ansvar for at virksomhetens sikkerhetsrutiner er kjent og etterleves, og at nødvendige vurderinger av risiko blir gjort og følges opp.
- Ledere bør sørge for at alle vet hvor man sier fra om bekymringer og sikkerhetshendelser, at man tar kontakt hvis noe «skurrer» eller hvis man ønsker å snakke om noe knyttet til sikkerhet i eget arbeid.

Bruk Sikresidens kursopplegg for ledere

Sikresiden utvikler ressurser som kan hjelpe ledere med å gjøre sikkerhet snakkbart og håndterlig, følge opp medarbeidere og tilrettelegge for nødvendige verdi- og risikovurderinger. Ledere bør gjøre seg kjent med ressurser fra Sikresiden. De kan brukes som utgangspunkt og underlag.

Virksomheten bør tilrettelegge for bevisstgjøring og erfaringsdeling ledere imellom. Sikresiden kan hjelpe til med å utvikle et tilpasset opplegg for den enkelte virksomhet.

1.5 Forskere må være aktsomme

Forskningsetiske vurderinger skal bidra til å beskytte forskningsdeltakere, forskernes integritet og forskningens samfunnsansvar. Forskere er også i en nøkkelposisjon til å gjøre nødvendige sikkerhetsmessige vurderinger med utgangspunkt i verdiene i egen forskning.

Universities have a key role in empowering researchers as active partners in safeguarding knowledge by providing clear responsibilities, targeted training, and recognition for their contributions to research security.

Research security as a collective responsibility: empowering universities, enabling Europe (s.3)

Aktsomhet betyr å være påpasselig og oppmerksom så man ikke påfører seg selv og andre skade, tap eller ulempe. Forskere i internasjonale kontaktflater og nettverk kan være særlig utsatt som direkte mål for fremmed etterretning og påvirkning. De må derfor ha handlingskompetanse til å opptre ansvarlig og motstandsdyktig i et krevende trusselbilde.

1.5.1 Om internasjonalt forskningssamarbeid

I en internasjonal forskningsfront kan forskere møte på sikkerhetsrelaterte og forskningsetiske problemstillinger og dilemma. Med gode undersøkelser og vurderinger, kan risiko identifiseres og håndteres, slik at samarbeid kan gjennomføres på en trygg måte.

Forskere og ledere bør diskuter hva som kan skje, hva som kan være utfordrende og hvordan de kan møte hendelser og utfordringer.

Hva er lurt å undersøke om samarbeidspartneren?

En «due diligence» er en undersøkelse av partnerens aktiviteter, sektoren den opererer i og en kommersiell og etisk vurdering av ledelse og rammer:

- Har partneren en spesiell agenda, politisk, ideologisk eller kommersiell, som bør hensyntas?
- Er partneren, inkludert ansatte eller personer i styrende organer knyttet til militær aktivitet eller selskaper med uklar profil?
- Hva slags forhold har partneren til sine egne myndigheter, nasjonale eller lokale?
- Hva slags beslutningsstrukturer har partneren?
- Er det noen saker eller hendelser som har skapt problemer med tidligere relasjoner eller utenlandske partnere?
- Forplikter partneren seg til å følge regler eller normer for etikk, transparens, åpenhet og akademisk frihet?
- Har partneren en sunn økonomi og gode og etterrettelige systemer for drift?

Les mer: Partnerskap på forskningsfeltet | HK-dir

Søk i åpne kilder

Web of Science (eller Scopus) og ORCID kan brukes i kombinasjon til å innhente informasjon om enkeltforskere over hele verden. Verktøyet kan brukes både til å finne interessante muligheter og å oppdage mulige kilder til risiko.

Les mer: Ansvarlig int. samarbeid: Kjenn din partner og fremtidige arbeidstaker | HK-dir

1.5.2 Reiser, konferanser og utenlandsopphold

Reiser og konferanser er vante arbeidsmiljø for mange forskere. På reise er man gjerne opptatt av faglige presentasjoner, samarbeid og viktig nettverksbygging. Kanskje er det vanskelig å vurdere hva som er normalt og hva som «skurrer».

> Konferanser kan være et arnested eller grobunn for utenlandsk etterretningsvirksomhet, hvor åpne eller fordekte tilnærminger fra utenlandske etterretningstjenester kan skje.
>
> *PST i Khrono 02.02.26*

Mange virksomheter har etablerte rutiner for sikkerhet på reise, konferanser og utenlandsopphold. Tema som bør dekkes i rutineverket kan være:

- grunnleggende sikkerhet
- IKT-sikkerhet på reise
- personlige gaver og invitasjoner
- særskilte rutiner for dem som er ekstra trusselutsatt

Forberedelser til konferanser og utenlandsopphold bør inkludere:

- Innhenting av informasjon om vertslandet, og kjennskap til lokale lover og skikker, inkludert forståelse av vertslandets holdning til akademisk frihet og åpen diskusjon.
- Vurdering av hvilken informasjon som deles eller presenteres, samt klare rammer for hvilke deler av forskningen som kan og ikke kan diskuteres.
- Avklaring av at eventuelle honorarer eller betalinger ikke skaper interessekonflikter eller medfører kontraktsbrudd eller brudd på universitetets retningslinjer.
- Rapportering av mistenkelig hendelse til nærmeste leder og riktig instans ved virksomheten.

Bruk Sikresidens opplæringsressurser for forskere

Sikresiden utvikler opplærings- og bevisstgjøringsressurser i forskningssikkerhet og ansvarlig internasjonalt samarbeid. Opplæringen skal blant annet hjelpe dem:

- identifisere og håndtere risiko knyttet til verdiene de forvalter i eget arbeid
- vurdere egne sårbarheter
- gjenkjenne røde flagg i egen hverdag
- si fra når noe «skurrer»

Bruk: E-læringene kan distribueres til forskere, gjerne i forkant av avdelingsmøter der problemstillingene blir fulgt opp. De kan også brukes som presentasjoner i møter eller seminarer og som underlag for gruppediskusjoner.

Sikresiden utvikler også opplæring og sjekklister knyttet til reiser, feltarbeid og utenlandsopphold samt reiser til risikoland.

1.6 Alle må si fra

Å si fra om noe er ikke en anklage. Å senke terskelen for å si fra om sikkerhetshendelser eller spørre om hjelp, er et av de viktigste sikkerhetstiltakene.

Virksomhetene må ha gode systemer for å

- melde fra om hendelser
- si fra om bekymringer og når noe «skurrer»
- spørre om hjelp

Systemer for å si fra bør være fleksible og ikke basert på at medarbeideren alltid bruker «riktig kanal». Den som sier fra bør informeres om hvordan bekymringen blir fulgt opp.

Hvordan håndtere en bekymring?
Både ledere, sikkerhetsroller og HR-medarbeidere bør kunne motta en bekymring og vite hvordan den skal håndteres videre.

Si fra til PST

PST har hovedansvaret for å hindre spionasje i Norge. De er avhengige av tips. Selv små observasjoner og pussige hendelser kan ha stor verdi for PST når de vurderer dette i sammenheng med annen informasjon de har.

Ved mistanke om spionasje, skal virksomhetene kontakte PST.

Enkeltpersoner kan også tipse PST. Det er trygt å tipse PST. Det får ingen konsekvenser for uskyldige, eller for den som sier fra. PST har ansvaret for videre oppfølging.

Les mer på Forebyggende: Spionasje | sikresiden.no

1.7 Bli kjent med Sikresiden

Virksomhetene bør samle personer i relevante roller, og lage en oversikt over opplæringsbehov, og oversikt over ressurser som møter disse behovene.

- Hvem trenger opplæring i hva?
- Hvor ofte?
- Hvilken opplæring gjennomføres per i dag?
- Hvilke ressurser trenger vi for å møte opplæringsbehovet?
- Hvilke ressurser har vi gjennom Sikresiden-samarbeidet?
- Kan vi illustrere dette i et hjul eller skjema?
- Hvem har ansvaret for de ulike opplæringstiltakene?

Bli kjent med Sikresiden og lag oversikt over opplæringsbehovet i virksomheten

Gjennom Sikresiden-samarbeidet har UH-sektoren utviklet lett tilgjengelige opplæringsressurser som dekker et bredt spekter av sikkerhetstema, til ulike målgrupper. De er klare til bruk, men kan også enkelt og kostnadsfritt tilpasses den enkelte virksomhet.

De kan distribueres til utvalgte ansatte via e-post, eller de kan danne utgangspunkt for fysiske kurs, møter eller seminarer. Ledere på alle nivåer bør gjøre seg kjent med Sikresiden og ressursene de har tilgjengelig der.

Basisopplæring i sikkerhet fra Sikresiden

Sikkerhetsopplæring er ferskvare. Den må oppdateres i forhold til endringer i trusselbildet og repeteres jevnlig.

Sikresiden vedlikeholder e-læringer om grunnleggende sikkerhetstema. Temalisten og innholdet revideres årlig og ved behov. Virksomhetene står fritt til å selv legge til eller trekke fra tema.

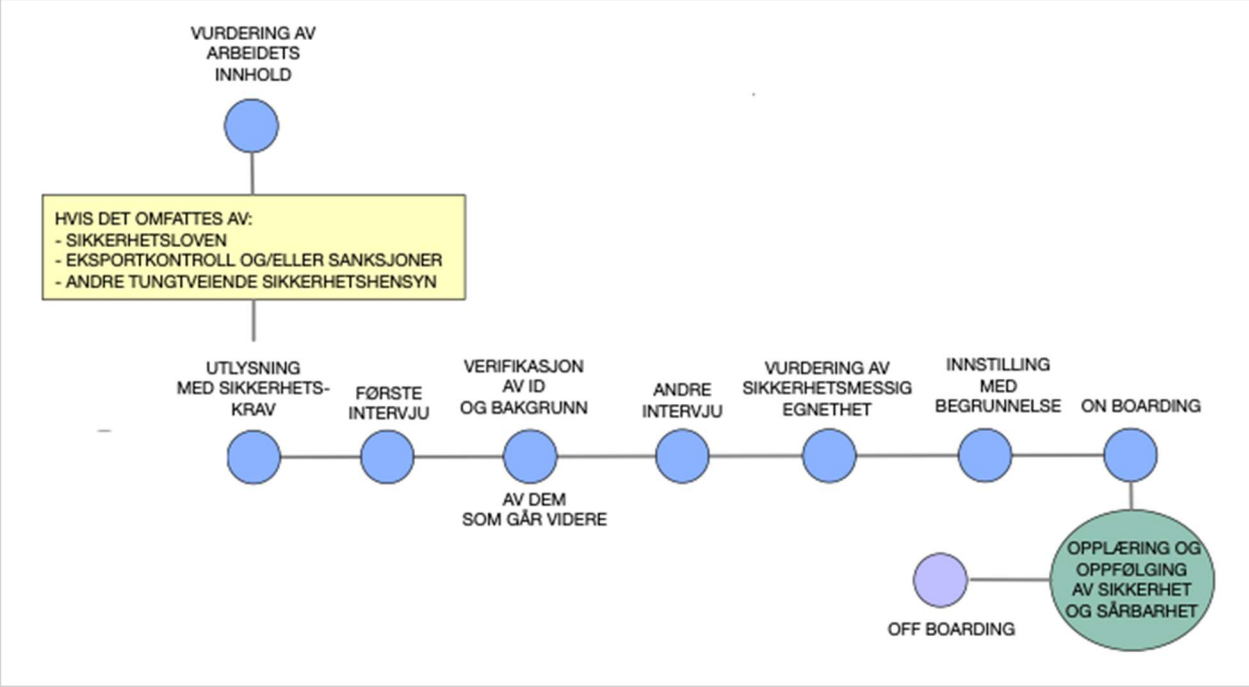
Bruk: Basisopplæringen i sikkerhet er velegnet som en del av mottak og introduksjonsprogram for nye medarbeidere. Alle eller utvalgte e-læringer kan også distribueres til alle ansatte ved behov, som for eksempel i etterkant av hendelser, som del av sikkerhetsmåned, kampanjer eller lignende.

Oversikt over opplæringsressurser fra Sikresiden: Opplæring i sikkerhet (sikresiden.no)

For dem som planlegger og tilrettelegger for opplæring: Slik bruker du ressursene fra sikresiden.no (sikresiden.no)

Tips: Digdir har en veileder i hvordan man planlegger opplæring og kompetansetiltak.

DEL 2 SIKKERHET I REKRUTTERING OG OPPFØLGING



Figur 1: Sikkerhet i rekruttering og oppfølging av personell

Denne delen baserer seg på en gjennomgang av regelverk, vurderingskriterier og risiko som finnes i del 4. Gjennomgangen konkluderer med å anbefale tre kategorier for vurdering av arbeidets innhold, som vil medføre ulike nivå av personellmessige sikkerhetskrav og oppfølging. Se til del 4 ved behov for mer utdypende informasjon.

Vurderinger og metoder presentert i denne delen er også relevante i andre prosesser, som for eksempel

- når forskere deltar i forskningsprosjekter med sikkerhetskrav
- ved interne overflytninger av medarbeidere fra et arbeidsområde til et annet
- når det gis midlertidige tilganger, som ved invitasjon og mottak av gjesteforskere og i uformelle forsker-til-forsker-samarbeid

2.1 Vurderinger før utlysning

Før utlysning av en stilling, bør ansettende leder med sin rådgivende gruppe foreta en stillings- og oppdragsspesifikk risikovurdering[6]. Dette bør gjøres som del av *jobbanalysen*.

2.1.1 Vurdering av arbeidets innhold

Vurder hvorvidt arbeidets innhold faller inn under en eller flere av disse tre kategoriene:

1. Arbeidet medfører tilgang til verdier som er sikkerhetsgradert og eller skjermingsverdig etter sikkerhetsloven.
2. Arbeidet medfører tilgang til verdier som er lisenspliktig etter eksportkontroll- og sanksjonsregelverket.
3. Arbeidet medfører tilgang til verdier med andre tungtveiende sikkerhetshensyn.

I tillegg er det nødvendig å vurdere følgende faktorer:

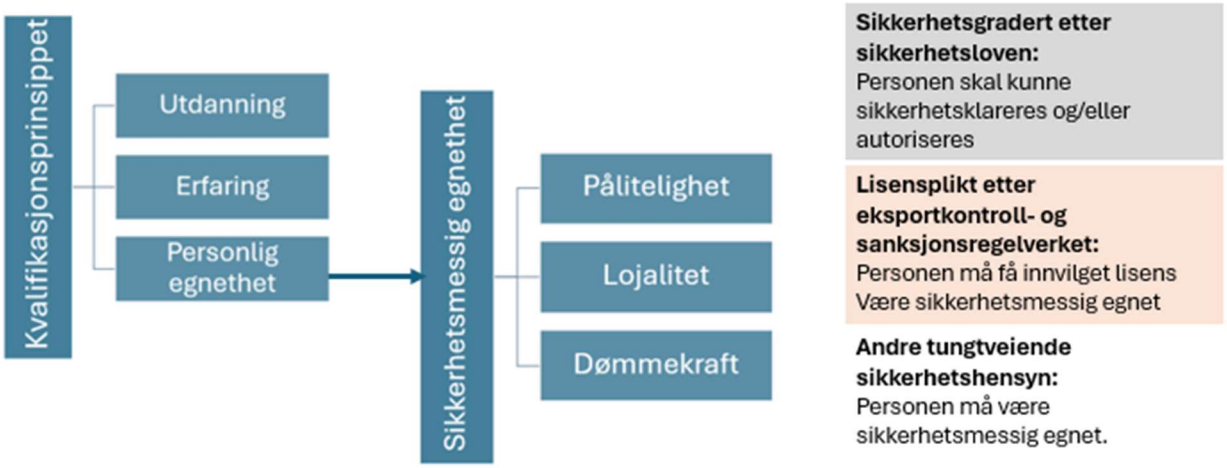
- Stilles det sikkerhetskrav fra samarbeidspartnere for denne stillingen?
- Er det en fast eller midlertidig stilling?
- Har stillingen et tydelig arbeidsinnhold, som et avgrenset prosjekt eller oppdrag, eller er det en stilling med stor autonomi og utviklingspotensial?
- Er det behov for rask oppstart, eller går det å vente på eventuelle nødvendige sikkerhetsklareringer eller lisenser?
- Listen over er ikke utfyllende. Diskuter om det også kan være andre forhold som er aktuelle.

Selv om arbeidet i den konkrete stillingen isolert sett ikke medfører særskilte sikkerhetsbehov, kan det aktuelle fagmiljøet med ressurser og infrastruktur i sin helhet vurderes som trusselutsatt. Andre miljø og faglige nettverk som stillingen gir tilgang til, kan også representere en totalverdi som bør vurderes ut fra et oppdatert trusselbildet. Hvor grundige undersøkelser og vurderinger man velger å gjennomføre, bør derfor være balansert med verdiene og risikoen totalt sett som er knyttet til arbeidets innhold.

[6] Foreta stillings- og oppdragsspesifikke risikovurderinger - Nasjonal sikkerhetsmyndighet

2.1.2 Vurdering av krav til personlig sikkerhetsmessig egnethet

Sikkerhetsmessig egnethet handler om en persons pålitelighet, lojalitet og dømmekraft i forhold til de verdiene personen skal forvalte i sitt arbeid. Dersom arbeidets innhold faller i en av de tre kategoriene, bør nivåkravet til personlig sikkerhetsmessig egnethet inkluderes i kvalifikasjonskravet, og komme tydelig frem av kunngjøringsteksten.



Figur 2: Kvalifikasjonsprinsnippet og krav til sikkerhetsmessig egnethet

Når det opplyses i utlysning av en stilling at arbeidet krever sikkerhetsklarering og/eller autorisasjon, innvilget lisens, eller vurdering av personlig sikkerhetsmessig egnethet, er søkeren informert om at nødvendig informasjon og personopplysninger må oppgis og innhentes til dette formålet.

2.2 Vurderinger i rekrutteringsprosessen

De tre kategoriene innebærer ulike nivåkrav til sikkerhetsmessig egnethet. De forskjellige nivåene innebærer også hvor omfattende slike undersøkelser skal være, og ulikhet i hvem som gjennomfører undersøkelsene og vurderingene.

Hvem gjør hvilke vurderinger?

1. **Sikkerhetsklarering og autorisasjon etter sikkerhetsloven**
   Sivil klareringsmyndighet gjennomfører personkontrollen for sikkerhetsklarering. Den autorisasjonsansvarlige i virksomheten gjennomfører autorisasjonssamtalen. Personkontrollen blir mer omfattende jo høyere

graderingsnivå. I enkelte tilfeller skal også Nasjonal sikkerhetsmyndighet involveres.

2. **Lisens og tillatelser etter eksportkontroll- og sanksjonsregelverket**
   DEKSA vurderer og behandler hver søknad om lisens og tillatelser individuelt. Arbeidsgiver må selv vurdere sikkerhetsmessig egnethet og definere tiltak.

3. **Sikkerhetsmessig egnethet av andre tungtveiende sikkerhetshensyn**
   Arbeidsgiver må selv vurdere sikkerhetsmessig egnethet og definere tiltak.

2.2.1 Hvordan vurdere personlig sikkerhetsmessig egnethet

Hvordan kan arbeidsgiver vurdere sikkerhetsmessig egnethet?

- **Sikkerhetsbevissthet og risikoerkjennelse**
  Dette handler blant annet om forståelse av risiko og holdninger til sikkerhetstiltak. Dette kan vurderes gjennom å stille litt åpne spørsmål for refleksjon over relevante tema, som stillingens arbeidsområde og trusselbildet, rutiner og tiltak som sikkerhet kan innebære i den aktuelle stillingen, og hvordan håndtere vanskelige situasjoner og dilemma.

- **Landtilknytning**
  Dette handler om å kunne håndtere risiko for blant annet kunnskapsspionasje, ved at en ansatt kan bli utsatt for press, fristelser eller andre former for tilnærminger fra fremmed etterretning. Det handler også om å kunne ivareta den ansatte.

- **Andre tilknytninger**
  Til alle stillinger med krav til personlig sikkerhetsmessig egnethet vil det være nyttig å undersøke personens sampubliseringer og annet vitenskapelig samarbeid, eventuelle næringsinteresser, finansieringsforbindelser, eller andre tilknytninger eller forbindelser som kan ha en betydning.

2.2.2 Bakgrunnssjekk og tilknytninger

For at virksomheten skal få et godt nok grunnlag til å vurdere *sikkerhetsmessig egnethet*, kan det være aktuelt å innhente mer informasjon om personens bakgrunn og tilknytninger. En slik bakgrunnssjekk kan gjennomføres ved ulike metoder og kilder.

Bruk kandidatens CV som en viktig informasjonskilde

- Informasjon i CV kan indikere knytninger det er verdt å undersøke nærmere.
- Hull i CV med manglende informasjon om utdanning eller arbeid, bør undersøkes.
- Enkelte kandidater kan utelate informasjon i CV for å ikke avsløre tilhørighet til hjemlandets myndighetsorgan eller annet.

Undersøk dokumentasjon og bakgrunn

- Fysiske dokumentet som vitnemål og attester bør fremlegges, og undersøkes av en som har kompetanse på hva man skal se etter. Mange ganger er det mulig å kontakte utsteder. Nasjonalt id-senter tilbyr tilgang til ulike databaser, ressurser og opplæring for offentlige virksomheter i verifikasjon av fysiske dokumenter.
- Undersøk forhold knyttet til vitenskapelig aktivitet og samarbeid, forskningsvirksomheter, finansieringskilder, sampublikasjoner. Web of Science (eller Scopus) og ORCID kan brukes i kombinasjon til å innhente informasjon om enkeltforskere over hele verden. Verktøyet kan brukes både til å finne interessante muligheter og å oppdage mulige kilder til risiko.

Funn det er ønskelig å undersøke nærmere:

Undersøkelsene kan avdekke uklarheter eller andre forhold det vil være nødvendig å følge opp med kandidaten. Be om mer informasjon og få avklart forhold av betydning, for eksempel uklarheter knyttet til:

- statsborgerskap og landtilknytninger
- tilknytninger til selskaper, næringsliv og eventuelle økonomiske samarbeid og bindinger

Det er også nyttig å bruke referansesamtalen(e) godt, også i et sikkerhetsperspektiv.

Når kan man innhente personopplysninger, og hva er lovlig behandlingsgrunnlag?
Å innhente personopplysninger i forbindelse med en bakgrunnssjekk må være nødvendig for å ivareta arbeidsgiverens legitime interesser. Opplysningene skal være relevante for å vurdere hvilken risiko personen kan utgjøre, knyttet til arbeidets innhold.

GDPR artikkel 6 nr. 1, bokstav f. om berettiget interesse

- Denne er lovlig dersom arbeidsgiver kan dokumentere at behovet for å gjennomføre en slik undersøkelse veier tyngre enn kandidatens vern av personopplysninger.
- Dette behandlingsgrunnlaget dekker ordinære personopplysninger, og ikke opplysninger i særlige kategorier etter GDPR artikkel 9.

GDPR artikkel 6 nr. 1, okstav b. om avtaleinngåelse eller avtaleoppfyllelse

- Dette grunnlaget dekker også særlige kategorier av personopplysninger, jf. personopplysningsloven § 6 og GDPR art. 9 nr. 2 bokstav b. Forutsetningen er at arbeidsgiver vurderer bakgrunnssjekken som en del av sine forpliktelser knyttet til å ansette den beste kandidaten til stillingen.

Åpenhet om kravene i utlysningsteksten fungerer som forventningsavklaring til kandidatene om hvor grundige bakgrunnsundersøkelser som vil bli foretatt i rekrutteringsprosessen. Det normalt kun lovlig å gjennomføre en bakgrunnssjekk av kandidatene som det er aktuelt å gi tilbud om ansettelse, og ikke av alle søkerne.

2.2.3 Kontroll av ID og oppholdskort

ID-kontroll og verifikasjon av ID-dokumenter er et helt grunnleggende tiltak ved enhver rekruttering eller midlertidig tilknytning.

Hva er et ID-dokument?
Et ID-dokument er et offisielt dokument som beviser hvem personen er. I Norge skal et ID-dokument inneholde bilde, fødselsnummer og være utstedt av en offentlig myndighet. Internasjonalt er det pass som oppfyller kravene.

Et ID-dokument har innebygde sikkerhetselementer som er til hjelp ved ekthetsvurderingen. Alle pass og nasjonale ID-kort fra EU/EØS har dette.

Hva slags ID-dokument skal en utlending som oppholder seg i Norge ha?
Les mer på Nasjonalt ID-senters nettsider.

Virksomheten er strafferettslig ansvarlig for at personell som skal arbeide og studere i Norge har lovlig opphold. For personer utenfor EU/EØS kreves det *oppholdstillatelse* i Norge (visum gjelder normalt kun for 90 dager i en 180 dagers periode).

Hva er et oppholdskort?
Et oppholdskort er en bekreftelse på at en person har lovlig opphold i Norge. Alle som har oppholdstillatelse i Norge, og ikke er EU/EØS-borgere skal ha et slikt kort. Det er et plastkort i bankkortstørrelse, med innebygde sikkerhetselementer til hjelp i ekthetsvurderinger. Oppholdskortet er ikke et ID-dokument.

Les mer på UDIs nettsider.

Dette sier politiet om hvordan man undersøker ID-dokumenter:

- Sjekk om dokumentet er skadet. Hvis det er skadet, må du vurdere om du kan godta det som ID-bevis.
- Kontroller informasjon på ID-beviset:
  - Se på utløpsdatoen, og at dokumentet ikke er utløpt.
  - Se på alle bildene, og se om de er like.
  - Navn og fødselsdato
- Når du har gjennomført dokumentkontrollen må du forsikre deg om at ID-beviset tilhører personen.
  - Se på bildet på dokumentet og på personen foran deg. Er det samme person?
  - Se på høyden som står på dokumentet. Stemmer denne med persons høyde?

- Spør gjerne om informasjonen du ser på dokumentet, for eksempel om personens alder.
- Hvis du er i tvil om dokumentet tilhører personen, bør du be andre om en annenhåndsvurdering.

Les mer på politiets nettsider

ID-kontroll ved rekruttering

- Kandidaten bør fremlegge ID-dokument og eventuelt oppholdskort ved fysisk oppmøte i løpet av rekrutteringsprosessen.
- Dersom kandidaten rekrutteres fra utlandet, bør virksomheten vurdere hvilke alternative metoder som er tilstrekkelige frem til vedkommende skal identifisere seg fysisk med originale dokumenter overfor norske myndigheter.
- ID-kontroll og kontroll av eventuelt oppholdskort må gjennomføres av virksomheten ved oppmøte, før vedkommende får adgangskort.

Nasjonalt ID-senter tilbyr nyttige ressurser og opplæring i ID-kontroll for offentlige virksomheter. Tjenestene er gratis.

Oversikt over opplæringstilbudet fra Nasjonalt ID-senter.

2.2.4 Bakgrunnssjekk fra tjenesteleverandører

Bakgrunnssjekk tilbys som en tjeneste fra flere kommersielle aktører. Det bør gjøres gode vurderinger av hva virksomheten kan gjøre selv, og hva man eventuelt kan kjøpe som en tjeneste.

Før kjøp av bakgrunnssjekk fra tilbydere, vurder dette:

- Basert på risiko: Hva trenger vi for å gjøre de nødvendige vurderingene?
- Hva er det leverandøren tilbyr som vi ikke kan gjøre selv?
- Hva er de økonomiske og administrative kostnadene veid opp mot virksomhetens sikkerhetsbehov og krav til kontroll?

Spørsmål som bør stilles ved vurdering av tilbydere av bakgrunnssjekk:

- Hvilke nasjonale og internasjonale verifikasjonskilder og kompetanse har de tilgang til og hvordan bruker de dem?
- Hvordan blir resultatene presentert?
- Hvilke krav til kompetanse og sikkerhetsmessig egnethet har de til egne ansatte, og hvilken sikkerhetsmessig oppfølging får de?
- Hvilke tredjepartsleverandører blir brukt, og hvilke krav stilles til dem?
- Hvis de tilbyr «sårbarhets- eller sikkerhetssamtaler», hvordan gjennomføres disse og hvilken dokumentasjon får virksomheten?
- Hvordan behandles og sikres personopplysningene?

2.3 Rekrutteringsprosessen når sikkerhetsloven gjelder

Når arbeidets innhold inkluderer verdier som er *sikkerhetsgradert* eller *skjermingsverdig* etter sikkerhetsloven, skal de behandles i henhold til lovens krav med tilhørende forskrifter. Den som ansettes må kunne sikkerhetsklareres og/eller adgangsklareres til nødvendig nivå, og/eller autoriseres av virksomheten.

Eksempler på verdier som er sikkerhetsgradert eller skjermingsverdige etter sikkerhetsloven, i UH-sektoren

- *Sikkerhetsgradert informasjon* som virksomheten behandler selv, eksempelvis i virksomhetens interne sikkerhetsorganisasjon. Dette vil i hovedsak være på nivå BEGRENSET (lavgradert, hvor kun autorisasjon og ikke sikkerhetsklarering er nødvendig) eller KONFIDENSIELL.

- *Sikkerhetsgradert informasjon* i forskning. Dette kan være i samarbeid med aktører som behandler sikkerhetsgradert eller skjermingsverdig informasjon, eller som har andre skjermingsverdige verdier regulert av sikkerhetsloven.
    - Forskningsprosjekter med finansiering fra Forskningsrådets nye portefølje for forsvarsevne, sikkerhet og beredskap[7] kan, basert på verdi- og skadevurdering til deler av prosjektet, komme til å bli helt eller delvis sikkerhetsgradert.

[7] Portefølje for forsvarsevne, sikkerhet og beredskap

- Ved deltakelse i EU-prosjekter med midler fra eksempelvis *European Defence Fund*[8] (EDF) eller andre tilsvarende prosjekter, kan det medfølge personellmessige sikkerhetskrav, særlig dersom deltakelse i prosjektet medfører behandling av EU Classified Information (EUCI).

EU stiller krav til klassifisering og behandling av informasjon som har sikkerhetsmessig skadepotensiale for EU eller for et eller flere EU-medlemsland. Slik klassifisert informasjon omtales som EUCI. Disse kravene er definert gjennom egne bestemmelser, og er bygget opp med fire nivå, lik NATOs klassifisering og den som følger av den norske sikkerhetsloven[9].

Det er utformet personellmessige sikkerhetstiltak for å sikre at tilgang til EUCI kun gis til de som har:

- et behov for informasjonen
- blitt sikkerhetsklarert til riktig nivå, der det er hensiktsmessig
- blitt informert om deres ansvar

Slike definerte krav må imøtekommes av virksomheter og den enkelte person som deltar i slike forskningsprosjekter.

Dersom det er samarbeidspartneren eller prosjekteieren som også er eier av den skjermingsverdige/sikkerhetsgraderte informasjonen, informasjonssystemet, objektet eller infrastrukturen, vil det også i hovedsak være samarbeidspartneren som er ansvarlig for å stille personellmessige sikkerhetskrav til forskere som skal delta i forskningssamarbeidet.

Til jobbanalysen: Vurderingskriterier for arbeidets innhold (Sikkerhetsloven)

- Arbeidets innhold medfører, eller vil med høy sannsynlighet medføre, utvikling av eller tilgang til *sikkerhetsgradert informasjon*.

[8] European Defence Fund (EDF) - Official Webpage of the European Commission. - Defence Industry and Space
[9] Council security rules for protecting classified information (EUCI) | EUR-Lex

- Arbeidets innhold medfører, eller vil med høy sannsynlighet medføre, utvikling av eller tilgang til informasjon som *er EU Classified Information*.
- Arbeidets innhold medfører, eller vil med høy sannsynlighet medføre, utvikling av eller adgang *til objekter eller infrastruktur som er vurdert som skjermingsverdige*.

Krav til sikkerhetsmessig egnethet: Forslag til tekst i utlysningen

Den som ansettes skal kunne sikkerhetsklareres og/eller autoriseres til «dette nivå» (B/K/H/SH).

Oppfølging i rekrutteringsprosessen og i arbeidsforholdet

Virksomheten undersøker følgende forhold i rekrutteringsprosessen, basert på metoder og informasjonsunderlag som er tilgjengelig og lovlig:

- Sikkerhetsbevissthet og risikoerkjennelse
- Landtilknytninger
- Andre tilknytninger
- ID-kontroll, verifikasjon av dokumentasjon og bakgrunn

Etter tilsetting må virksomheten sende søknad om sikkerhetsklarering.

- Personen kan ikke få tilgang til sikkerhetsgradert informasjon eller andre skjermingsverdige verdier med krav til klarering, før nødvendig sikkerhetsklarering, eller adgangsklarering, og autorisasjon er gjennomført.
- Vurder om personen kan tiltre stillingen i en tidsavgrenset periode, og uten tilgang til sikkerhetsgradert informasjon eller andre skjermingsverdige verdier. Det bør tas inn i arbeidsavtalen at nødvendig klarering og autorisasjon er et vilkår for at ansettelsen kan opprettholdes.
- Den som ansettes skal ha opplæring og oppfølging i kravene for behandling av slike skjermingsverdige verdier. Disse må spesifiseres i virksomhetens interne rutiner for nasjonal sikkerhet.

2.3.1 Autorisasjonssamtaler

Autorisasjonssamtalen er et viktig verktøy for autorisasjonsansvarlig i virksomheten som et ledd i arbeidet med forebyggende sikkerhet.

Hensikten er å avklare om den autorisasjonsansvarlige i virksomheten har nødvendig tillit til at personen vil håndtere sikkerhetsgradert informasjon eller skjermingsverdig objekt og infrastruktur i henhold til lov, forskrifter, instruks og lokalt regelverk, og at personen er sikkerhetsmessig skikket. Samtalen vil også gi autorisasjonsansvarlige viktig informasjon om medarbeiderens pålitelighet, lojalitet og dømmekraft.

Det er viktig å forebygge at autorisasjonen ikke blir redusert til en formalitet. Den som er autorisasjonsansvarlig i virksomheten:

- Har et løpende ansvar for sikkerhetsmessig skikkethet også etter at autorisasjonen er gitt. Dette innebærer at ny vurdering må finne sted om det oppstår forhold som kan ha betydning for sikkerheten.
- Skal vurdere om tiltak kan redusere risiko på slik måte at autorisasjon kan opprettholdes, om autorisasjonen må suspenderes, gis til et lavere nivå eller opprettholdes.
- Plikter å varsle klareringsmyndigheten når dette er nødvendig på samme måte som at medarbeider er pliktig til å opplyse om forhold som kan påvirke egen sikkerhetsmessig skikkethet.

Dokumentasjon av opplysningene sammen med andre personkontrollopplysninger i sikkerhetskonvolutten vil være viktig for senere oppfølging, ved bytte av autorisasjonsansvarlig, om nye forhold oppstår eller for å kunne gi ytterligere opplysning om håndterte forhold i klareringsperioden ved reklarering.

Sikkerhetsloven stiller ulike krav for autorisasjon til nivå BEGRENSET og autorisasjon til nivå KONFIDENSIELT eller høyere. For eksempel vil autorisasjon til nivå BEGRENSET for en utenlandsk statsborger som kommer fra en stat som Politiets sikkerhetstjeneste (PST) mener utgjør en høy sikkerhetsrisiko for Norge, medføre at den autorisasjonsansvarlige må innhente samtykke fra Sivil klareringsmyndighet.

Autorisasjonen bortfaller om personen slutter i stillingen, behovet for autorisasjon ikke lenger er til stede, eller om man ikke lenger har gyldig sikkerhetsklarering.

2.3.2 Sikkerhetssamtaler

Klareringsmyndigheten kan kalle inn til sikkerhetssamtaler i forbindelse med behov for ytterligere opplysninger i vurdering av klareringssak eller i klagesaksbehandling etter klareringsavgjørelse. Dersom det fremkommer opplysninger i klareringssaken som medfører tvil om en person er sikkerhetsmessig skikket, kan personen bli innkalt til en sikkerhetssamtale, jf. sikkerhetsloven § 8-4 tredje ledd og klareringsforskriften § 19.

Sikkerhetssamtalen er altså et saksbehandlingskritt som har til hensikt å opplyse klareringssaken tilstrekkelig, slik at riktig avgjørelse kan fattes.

Sikkerhetssamtalen understøtter dermed også individets rett til å kunne forklare seg om egne forhold som kan ha betydning for sikkerheten. Slik utgjør sikkerhetssamtalen et viktig rettssikkerhetsmessig prinsipp. Sikkerhetssamtalen kan også ha betydning for notoritet og etterprøvbarhet i saksbehandlingen ved klager eller tilsyn med klareringsinstituttet. Det er ingen plikt til å møte til sikkerhetssamtale, men en nektelse eller unnlatelse vil kunne tale negativt ved vurdering av klareringssaken, jf. sikkerhetsloven § 8-4 fjerde ledd bokstav j.[1]

2.4 Rekrutteringsprosessen når eksport- og sanksjonsregelverket gjelder

Når arbeidets innhold inkluderer verdier som er omfattet av eksportkontroll- og sanksjonsregelverket, utløses krav om lisens for alle som ikke har norsk statsborgerskap, dersom unntaksbestemmelsene ikke gjelder. Dersom kravet om lisens er utløst, søker man DEKSA om dette. Eventuell lisens er knyttet til en bestemt person. Kravet om lisens gjelder både ved

- ansettelse i fast eller midlertidig stilling
- ved intern overføring
- ved mottak av gjesteforskere eller annen vitenskapelig tilknyttet person

Til jobbanalysen: Vurderingskriterier for arbeidets innhold (Eksportkontroll- og sanksjonsregelverket)

- Vurder om arbeidets innhold medfører, eller med høy sannsynlighet vil medføre, behandling av flerbruksvarer eller teknologi som er oppført i Liste II eller Liste III til eksportkontrollforskriften.
- Vurder om arbeidets innhold medfører behandling av varer som er oppført i sanksjonslister til de enkelte sanksjonerte land[10].
- Forstå teknologinotene til de ulike varekategoriene og hvordan kontrolltiltakene i regelverket faktisk utløses.
- Vurder unntaksbestemmelsene, og den såkalte «fang-alt»-paragrafen
- DEKSA[11] kan kontaktes for råd og veiledning.

Krav til sikkerhetsmessig egnethet: Forslag til tekst i utlysningen

Den som ansettes må få innvilget nødvendig lisens eller tillatelse til å behandle eksportkontrollerte flerbruksvarer og teknologi, eller varer oppført på sanksjonslister til de enkelte land. Statsborgerskap må derfor oppgis. Ansettelse forutsetter at kandidaten vurderes som personlig sikkerhetsmessig egnet. I den forbindelse vil det også gjennomføres identitetskontroll og verifikasjon av dokumentasjon og bakgrunn av aktuelle kandidater.

Oppfølging i rekrutteringsprosessen og i arbeidsforholdet

Virksomheten undersøker følgende forhold i rekrutteringsprosessen, basert på metoder og informasjonsunderlag som er tilgjengelig og lovlig:

[10] Gjeldende sanksjoner – DEKSA
[11] https://deksa.no/eksportkontroll/trenger-du-lisens/kunnskapsoverforing/

- Sikkerhetsbevissthet og risikoerkjennelse
- Landtilknytninger
- Andre tilknytninger
- ID-kontroll, verifikasjon av dokumentasjon og bakgrunn

Etter tilsetting må virksomheten søke lisens til DEKSA.

- Personen kan ikke få tilgang til de regulerte verdiene før nødvendig lisens er innvilget.
- Vurder om personen kan tiltre stillingen i en tidsavgrenset periode og med reduserte tilganger, og med vilkår om at arbeidsavtalen vil opphøre dersom nødvendig lisens eller tillatelse ikke oppnås
- Dersom DEKSA ikke fatter klart vedtak, kan ansvarlig leder beslutte at personen likevel kan utføre det planlagte arbeidet, basert på en vurdering av risiko med tilhørende tiltak for å redusere den til et akseptabelt nivå.

Personen som ansettes skal ha opplæring og oppfølging som er nødvendig for å oppfylles forpliktelsene knyttet til lisensen som er gitt. Disse må spesifiseres i virksomhetens intern rutiner.

Personen som ansettes eller som utfører arbeidet, skal også ha opplæring og oppfølging, og i enkelte tilfeller følge virksomhetens rutine for sårbarhetsvurdering- og oppfølging.

2.5 Rekrutteringsprosessen når tungtveiende sikkerhetshensyn gjelder

Mange UH-virksomheter behandler verdier som skal beskyttes uten at de er direkte regulert i lovverk. I blå boks finnes eksempler på områder som kan omfattes av andre tungtveiende sikkerhetshensyn. Eksemplene er basert på trusselbildet i 2026 og hvilke verdier som er av strategisk betydning for Norge. En slik oversikt må holdes oppdatert.

Forskning, utvikling, og informasjon som kan innebære tungtveiende sikkerhetshensyn:

- som omhandler forhold av betydning for landets forsvar, totalforsvar, samfunnssikkerhet og beredskap, men som ikke er sikkerhetsgradert
- som representerer særlig stor verdi for landets utviklingsevne og økonomi
- som utreder grunnlag for nasjonale handlingsplaner og politikkutforming av interesse for andre stater
- som utvikles gjennom tilgang til avanserte laboratoriefasiliteter, eller andre avanserte objekter og infrastruktur
- som vil komme til anvendelse for tilbydere av samfunnskritiske tjenester eller digitale tjenester eller som avdekker oversikt over samfunnskritisk infrastruktur som kan misbrukes i sabotasjesammenheng
- innen sensitive teknologier, og informasjon om disse, risikovurdert ut fra delleveranse 4 i KVAST[11]
- som omhandler havet, havbunnen, kysten, nordområdene, Arktis og Svalbard
- som omhandler satelitt-teknologi, militær aktivitet og infrastruktur i verdensrommet
- innenfor helse og medisin som behandler store mengder helsedata og personopplysninger, og/eller som utvikles gjennom tilgang til avanserte laboratoriefasiliteter, eller andre avanserte objekter og infrastruktur
- innenfor samfunnsvitenskap og humaniora som behandler store komplekse datasett om den norske befolkningen og det norske samfunnet

- med tematikk som i enkelte land er kontroversielle, utsettes for påvirkning eller innblanding, er sensurert eller forbudt
- som gir kunnskapsgrunnlag for politiske beslutninger
- som har verdi og sikkerhetskrav som er definert av samarbeidspartner
- Annet: Teknisk-/administrative stillinger med særlig store/utvidede tilganger/myndigheter/rettigheter, som tilganger til store mengder personopplysninger, administratorrettigheter og budsjettmyndighet og enkelte lederstillinger, såkalte høyrisikoroller

Til jobbanalysen: Vurderingskriterier for arbeidets innhold (tungtveiende sikkerhetshensyn)

Virksomhetene må selv vurdere om verdiene som inngår i arbeidets innhold kan være utsatt for særskilt sikkerhetstruende virksomhet, og må beskyttes av tungtveiende sikkerhetshensyn, selv om dette ikke er regulert direkte av lov.

- Ta utgangspunkt i virksomhetens og/eller enhetens verdivurderinger, gjerne målt opp mot den angitte oversikten over. Bruk aktivt de årlige trussel- og risikovurderingene fra Politiets sikkerhetstjeneste, E-tjenesten og Nasjonal sikkerhetsmyndighet. Verdier som inngår i arbeidets innhold må vurderes opp mot forholdene som beskrives i disse rapportene.
- Vurder risiko for ulike typer uønskede hendelser som rammer verdiene. Ved å identifisere mulige hendelser, og vurdere aktualitet og risiko ved institutt-, fakultets eller virksomhetsnivå, kan man få bedre oversikt over hvilke stillinger som kan være utsatt.
- Dette gjelder både vitenskapelige stillinger, enkelte teknisk- administrative stillinger, og noen lederstillinger. Slike vurderinger gir et dokumentert grunnlag å vurdere sikkerhetsmessig egnethet i rekrutteringsprosesser, og behov for særskilt sikkerhetsmessig oppfølging.

- Forslag til metode for å vurdere risiko for uønskede innsidehendelser gis i del 3 i veilederen.

Krav til sikkerhetsmessig egnethet: Forslag til tekst i utlysningen

Ansettelse forutsetter at kandidaten vurderes som personlig sikkerhetsmessig egnet. I den forbindelse vil det også gjennomføres identitetskontroll og verifikasjon av dokumentasjon og bakgrunn av aktuelle kandidater.

Oppfølging i rekrutteringsprosessen og i arbeidsforholdet
I løpet av rekrutteringsprosessen bør virksomheten dokumentere og vurdere følgende

- Sikkerhetsbevissthet og risikoerkjennelse
- Landtilknytninger
- Andre tilknytninger
- ID-kontroll, verifikasjon av dokumentasjon og bakgrunn
- Kredittsjekk (i enkelte tilfeller)

Gjør en helhetlig og individuell vurdering:

- Hvilke risikoer kan arbeidet innebære?
- Hvordan kan disse eventuelt reduseres?
- Hvordan vurderes personens sikkerhetsmessige egnethet?
- Hva er leders muligheter for å følge opp og ivareta personen gjennom ansettelsesforholdet?
- Hvor avgjørende blir eventuell ikke akseptabel risiko for utøvelsen av arbeidet?

➢ Risiko bør også vurderes opp mot nytten av personens kompetanse, erfaringer og øvrige egenskaper.

- Dersom det gjelder en allerede ansatt person, kan arbeidsgiver gjennom sin styringsrett beslutte hvilke arbeidsområder den ansatte skal ha, og ikke ha.
- Personen som ansettes eller som utfører arbeidet, skal ha opplæring og oppfølging, og i enkelte tilfeller følge virksomhetens rutine for sårbarhetsvurdering- og oppfølging.

2.6 Sikkerhetsvurderinger og forholdet til diskrimineringsvernet

Sikkerhetsvurderinger må imøtekomme krav til diskrimineringsvernet.
En kandidat som regnes som best hva gjelder faglige og erfaringsmessige kvalifikasjoner, kan etter en helhetlig og individuell vurdering likevel representere en risiko som ikke kan håndteres med tilgjengelige tiltak.

Dersom den ikke akseptable risikoen omhandler *vernede egenskaper*, som eksempelvis *etnisitet*, kan det regnes som diskriminering etter likestillings- og diskrimineringsloven § 30 og § 9.

Dette må vurderes og dokumenteres opp mot diskrimineringsvernet (ldl § 9)

Forskjellsbehandling er bare tillatt hvis egenskapen det forskjellsbehandles på har **avgjørende betydning for utøvelsen av arbeidet** eller yrket, og når alle disse tre vilkårene er oppfylt:

1. **Forskjellsbehandlingen har et saklig formål**
    - Hvordan er arbeidets innhold vurdert som særlig utsatt for sikkerhetstruende virksomhet ifølge nasjonale trusselvurderinger, sektorvurderinger og risikovurderinger gjort av virksomheten selv og det aktuelle miljøet?
    - Hvilke sikkerhetsmessige vurderinger og krav knyttet til personell har eventuelle samarbeidspartnere som del av sin risikostyring, som må imøtekommes?

2. **Forskjellsbehandlingen må være nødvendig for å oppnå det konkrete formålet**

- Hvordan er forskjellsbehandlingen nødvendig for å redusere risiko tilstrekkelig?
- Hvordan er andre risikoreduserende tiltak for personinngripende, kostbare og vanskelig å gjennomføre?
- Tiltak ovenfor andre personer som kan berøres av risiko som kan følge av ansettelsen vil være utenfor arbeidsgivers rekkevidde å gjennomføre.

3. **Forskjellsbehandlingen skal ikke være uforholdsmessig inngripende overfor den/de som forskjellsbehandles**
   - Hvordan vektes de mulige ønskede effektene forskjellsbehandlingen har for å redusere risiko, med de eventuelle negative konsekvenser for den eller de som forskjellsbehandles?

2.7 Sikkerhetsoppfølging gjennom arbeidsforholdet

Felles for alle som jobber eksportkontrollregulerte verdier, eller verdier med tungtveiende sikkerhetshensyn, er at de kan være mål for etterretningsaktører eller andre som ønsker å utnytte deres tilganger til disse verdiene. Personellsikkerheten må opprettholdes gjennom arbeidsforholdet, ikke bare i rekrutteringsprosessen[12].

2.7.1 Forebyggende samtaler

De ansatte må ha god nok forståelse for hvordan de kan være utsatt for trusselbildet, og hvordan de kan si fra.

Hva er en forebyggende samtale?

- En forebyggende samtale adresserer nasjonale og internasjonale trusselvurderinger generelt og trusselbildet som er relevant for virksomheten spesifikt.
- Enkelte medarbeidere kan være spesielt utsatt enten på pga. sin funksjon, pga. sin bakgrunn eller andre forhold knyttet til jobben eller privatlivet.
- Samtalen kan gjennomføres individuelt eller i grupper.
- Samtalen kan involvere leder, sikkerhetsrådgiver, tillitsvalgte, eller andre.

[12] Grunnprinsipper for personellsikkerhet .pdf (s.11)

Noen kaller dette sårbarhetssamtale, andre kaller det bevisstgjøringssamtale.
Les mer her: Veileder-i-sarbarhetssamtaler.pdf

2.7.2 Oppfølgingssamtaler

Ledere bør kjenne til eventuelle forhold eller sårbarheter ved sine medarbeidere som kan bli forsøkt utnyttet, og følge opp på en god måte som ivaretar de ansatte og beskytter verdiene.

Forhold som bør følges opp av leder, kan for eksempel være:

- en uønsket hendelse
- endring i trusselbildet som særlig berører enkelte
- likegyldighet eller motstand til sikkerhetsrutiner
- endring i forbindelse med fravær, atferd eller arbeidsutførelse
- sårbarheter som trenger individuell oppfølging, som uttalt misnøye, rusproblemer, økonomiske vansker, spillavhengighet, livskriser eller samarbeidsutfordringer

En oppfølgingssamtale bør planlegges godt. Samtalen må oppleves trygg, både for medarbeideren og lederen. Lederen må blant annet være forberedt på at sensitive opplysninger kan bli delt i fortrolighet.

Informer medarbeideren godt om for eksempel

- at formålet er å ivareta den enkelte medarbeider og virksomhetens verdier
- hvem som deltar i samtalen
- at det er mulig å invitere med tillitsvalgt
- hvordan det som deles blir behandlet, beskyttet og eventuelt fulgt opp

2.7.3 Endringer i arbeidsforholdet

Ansatte vil i mange tilfeller få endret arbeidsområde og eller arbeidsoppgaver underveis i ansettelsen. Da er det viktig at man gjør en ny vurdering av arbeidets innhold og nye risikovurderinger knyttet til dette. Endringer i arbeidets innhold som innebærer endringer av tilganger, lokaler, mennesker eller fagmiljø, bør behandles som nyansettelser.

Endringer i arbeidet på grunn av sikkerhetsmessige forhold

Kontrolltiltak kan være

- begrensning av tilganger
- restriksjoner på reiser og andre aktiviteter
- andre tiltak som oppleves som kontrollerende eller begrensende

Arbeidsmiljølovens kapittel 9 sier at dersom det av sikkerhetsmessige årsaker er behov for å iverksette slike tiltak overfor en medarbeider, må det ha en saklig grunn og ikke innebære en uforholdsmessig belastning for den ansatte.

Det er viktig med godt samarbeid med de tillitsvalgte, og drøfte behov for tiltak, og utforming og gjennomføring av kontrolltiltak.

Arbeidsgiver er også pliktig å gi medarbeideren god informasjon om formålet med kontrolltiltak, praktiske konsekvenser for tiltaket og hvor lenge det skal vare.

2.8 Avslutning av arbeidsforholdet

Avslutning av et arbeidsforhold kan innebære en risiko for verdier som forskningsdata, upubliserte resultater, personopplysninger og systemtilganger.

Hvordan avslutte et arbeidsforhold

- Ha rutine for innlevering av utlevert utstyr
- Utarbeid sjekklister for fjerning av
  - tilgang til informasjon og systemer
  - adgang til fysiske objekter og infrastruktur
- Innfør rutiner for særskilt oppfølging ved konfliktfylte avslutninger

- Avklar eierskap og tilgang til forskningsdata etter fratreden.
- Gjennomfør avslutningssamtale med medarbeideren, der det blant annet tas opp at taushetsplikten også gjelder etter avslutning av arbeidsforholdet.

OBS! Universitets- og høgskolesektoren har mange midlertidige tilknytninger, som ofte faller utenfor ordinære HR-prosesser, men som likevel kan ha omfattende tilganger. Det må også utarbeides rutiner for hvordan disse behandles.

DEL 3 SYSTEMATISK ARBEID MED PERSONELLSIKKERHET

Denne delen handler om hvordan etablere og videreutvikle et systematisk arbeid med personellsikkerhet, ved å innlemme personellsikkerhet i sikkerhetsstyringen, og i HR-prosessene gjennom retningslinjer og rutiner. Dette er viktig både for å ivareta risikobasert tilnærming, og for en forsvarlig likebehandling av personellet.

3.1 Organiser og planlegg arbeidet

Ledelsen må beslutte å etablere et system for personellsikkerhet, og beslutte hvem som skal lede og koordinere arbeidet. Dedikerte personer med ulike kompetanser og funksjoner bør samarbeide for å ivareta det sikkerhetsfaglige, personellmessige og juridiske på en god og balansert måte. Personellsikkerhet vil kunne medføre opplevelse av endringer i arbeidsforholdet, og derfor er god medvirkning og kommunikasjon også helt nødvendig.

Anbefaling til hvordan

Forslag til hvem som bør delta i arbeidet og involveres:

- Sikkerhetsleder eller informasjonssikkerhetsleder, og sikkerhetsrådgiver
- HR-funksjoner og HR-ledelse
- Personell med juridisk kompetanse og personvernrådgiver
- Kommunikasjonsrådgiver
- Tillitsvalgte, vernetjenesten, redelighetsutvalg og lederlinjen må involveres

Lag en plan for utviklingsarbeidet som omfatter:

- Hvordan identifisere og kartlegge overordnet innsiderisiko
- Hvordan få personellsikkerhet inn i sikkerhetsstyringen og HR-prosessene
    - Finn ut hva det er viktig å få på plass ut fra hva dere mangler eller trenger å forbedre.
    - Få oversikt over eksisterende HR-prosesser og hvor det er naturlig å få inn personellsikkerhet

- Planlegg hvordan dere lagrer godkjente rutiner og dokumenter, og hvordan de skal publiseres og gjøres kjent.

- Vurder også hva som kan implementeres tidlig, fortløpende, og hva som bør vente til andre deler er mer ferdig
- Lag en kommunikasjonsplan for utvikling og implementering.
- Sørg for å presentere/ gi opplæring innen nye personellsikkerhetsrutiner og tiltak inn i eksisterende HR-prosesser og -systemer.

3.2 Identifiser og kartlegg risiko

NSMs kategori 2 **Beskytte**[13] utdyper:
«Denne kategorien omhandler **identifisering og kartlegging av risiko** knyttet til stillinger, oppdrag og rekruttering av nye medarbeidere. Dette er vurderinger som krever kunnskap om virksomhetens verdier og ressurser. Kategorien har derfor en sterk forbindelse til virksomhetens sikkerhetsstyring, og må sees i sammenheng med virksomhetens overordnede verdi-, trussel- og sårbarhetsvurderinger. Disse danner grunnlaget for mer konkrete risikovurderinger knyttet til personellsikkerhet.»

3.2.1 Hva er innsiderisiko

Risikovurderinger knyttet til personellsikkerhet handler om å vurdere risiko som ansatte, gjesteforskere og andre tilknyttede (personell) kan representere *ved sin tilgang til verdier* som skal beskyttes av sikkerhetsmessige hensyn. Dette omtales som *innsiderisiko*. NSM sine *Grunnprinsipper for personellsikkerhet*[2], og *Temarapport Innsidere*[3], konkretiserer innsiderisiko som følger:

Innsiderisiko oppstår med bakgrunn i

- *verdiene* virksomheten eller staten forvalter
- en kombinasjon av menneskelige, virksomhetsspesifikke og/eller andre *sårbarheter*

[13] Grunnprinsipper for personellsikkerhet .pdf

- det overordnede *trusselbildet* som til enhver tid møter Norge og den aktuelle virksomheten

En innsidehendelse skjer når

- en ansatt eller tilknyttet utsetter virksomheten for skade, misbruk eller tap.
  - *Den som er ubevisst* kan være uoppmerksom, eller bli utnyttet av andre uten at en selv forstår det.
  - *Den som er bevisst* kan være selvmotivert, eller ha blitt rekruttert eller presset av andre, eller personen kan være en profesjonell infiltratør.

FFI-rapporten *Hva vet vi om innsiderisiko*[14] fra 2023 utdyper gråsoner mellom den bevisste og den ubevisste «innsideren». Den omtaler også faktorer som reduserer innsiderisiko, som sikkerhetsmessige egnethet, betydningen av jobbtilfredshet, og sikkerhetsbevissthet. Den peker også på et stort behov for mer nasjonal forskning på ulike deler av personellsikkerhet.

En metastudie om innsidetrusselen utarbeidet av SINTEF Digital i 2023[15] sier at dette er et stort felt som rommer alt fra fysisk industrispionasje, cybertrusler og uoppmerksomme ansatte. Den peker på at definisjonene som brukes om innsidetrusselen sier lite om dynamikkene mellom individ og gruppe, individ og organisasjon og mellom de som er på innsiden og utsiden av virksomheten. Metastudien viser til at en *hendelsesbasert tilnærming* er en god metodikk for å vurdere og følge opp innsiderisiko. Gjennom en slik tilnærming kan aktuelle uønskede hendelser (scenarier) identifiseres, og bli gjenstand for risiko- og sårbarhetsanalyse (ROS).

3.2.2 Hendelsesbasert tilnærming

Beredskapsrådets *Veileder i risiko- og sårbarhetsanalyser for kunnskapssektoren*[16] gir en fullstendig, faglig og praktisk innføring i alle fasene i en overordnet risiko- og sårbarhetsanalyse (ROS), inkludert identifisering av uønskede hendelser.

[14] https://www.ffi.no/aktuelt/blogg/vi-ma-prioritere-personellsikkerhet
[15] https://www.sintef.no/publikasjoner/publikasjon/2246391/
[16] Veileder i risiko- og sårbarhetsanalyser for kunnskapssektoren | Universitetet i Stavanger

Forenklet sett følger denne veilederen tradisjonelle steg i en hendelsesbasert tilnærming hvor vi spør oss:

- Hva kan gå galt?
- Hva er årsakene til at det kan gå galt?
- Hva kan vi gjøre for å hindre at det skjer?
- Hva kan konsekvensene bli?
- Hva kan vi gjøre for å redusere konsekvensene dersom det skjer?

Som et bakteppe for å identifisere aktuelle innsidehendelser, anbefales det å studere de årlige nasjonale trussel- og risikovurderingene, forstå hvordan trusselaktørene opererer, og se hvordan egne verdier i forskningsmiljø og støttetjenester er eksponert for dette trusselbildet.

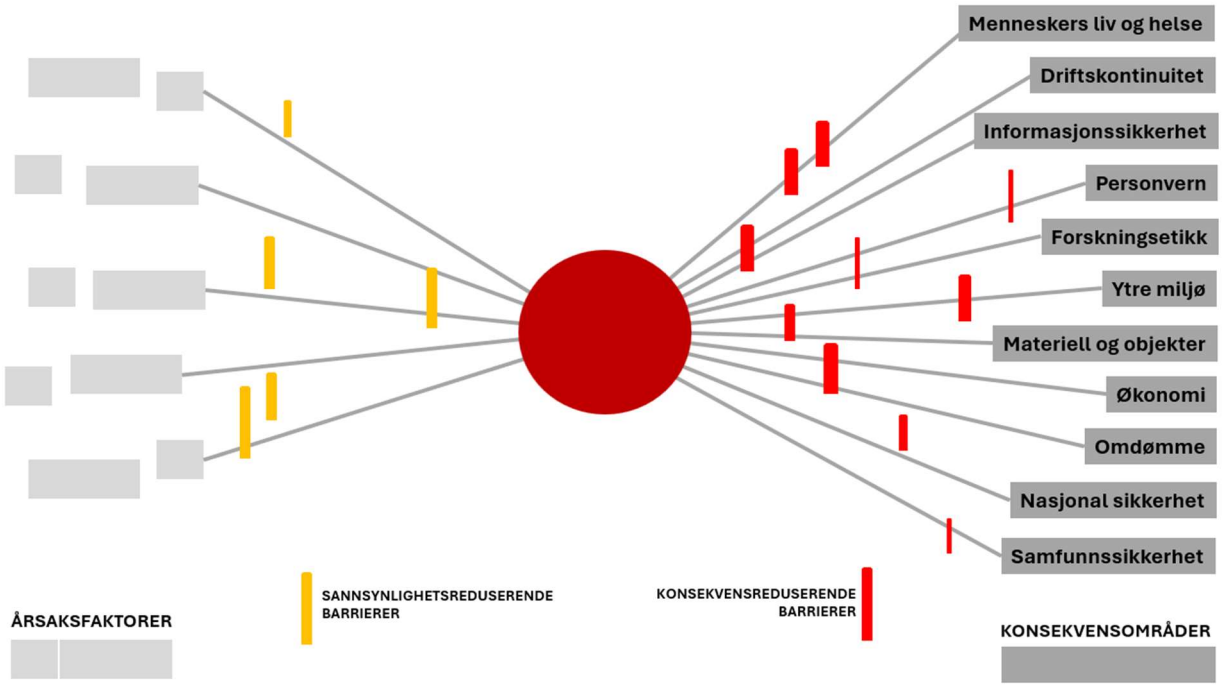
Dersom virksomheten har en faglig profil som er trusselutsatt, bør den utarbeide og jevnlig oppdatere egne trusselvurderinger. Egne trusselvurderinger bør knyttes sammen med de berørte enhetenes verdivurderinger og oversikt over fagområder som er særlig utsatt for sikkerhetstruende virksomhet. Dette vil være viktige grunnlag for gjennomføringen av personellmessige sikkerhetstiltak.

Anbefaling til hvordan

Kartlegging av virksomhetens risiko for innsidehendelser bør innlemmes i det kontinuerlige arbeidet med overordnede risiko- og sårbarhetsanalyse.

Gjennom en *hendelsesbasert tilnærming* vurderes sannsynlighet og konsekvens for identifiserte uønskede innsidehendelser.

Tiltakene som skal håndtere risiko bør utformes som del av systemet for personellsikkerhet, og være målrettet og dimensjonert forholdsmessig.



Figur 3: Sløyfediagram som illustrerer sammenheng mellom ulike innganger til en uønsket hendelse, og hvilke konsekvensområder en hendelse kan ramme, både for den enkelte ansatte, for virksomheten, og på et nasjonalt nivå.

Innsidehendelser i UH-sektoren

Det finnes kjente eksempler på *faktiske innsidehendelser* i norsk UH-sektor. Innsidehendelse i form av *kunnskapsspionasje* er fremhevet som et aktuelt scenario i HK-dir sin tilstands- og risikovurdering for 2025[17], med en sannsynlighet på 4 – Sannsynlig, for UH-virksomheter med trusselutsatte verdier.

Bruk Sikresiden

- Sikresiden har utviklet et støttemateriell til bruk for ROS som gir hjelp til å analysere *allerede identifiserte uønskede hendelser*, og består av

- Sikresiden har utarbeidet ulike typer relevante scenario, og eksempler på innsidehendelser

[17] Tilstands- og risikovurdering 2025 | HK-dir

3.3 Få personellsikkerhet inn i sikkerhetsstyringen og HR-prosessene

Nasjonal sikkerhetsmyndighet sitt grunnprinsipp 2.1 sier at personellsikkerhet bør integreres i sikkerhetsstyringen (s. 8)[18].

Personellsikkerhet bør inngå som en integrert del av virksomhetens helhetlige sikkerhetsstyring. Det menneskelige aspektet ved sikkerhet bør prioriteres av og forankres hos ledelsen. Dette krever en systematisk tilnærming som blant annet omfatter fagkompetanse, ressurser, rutiner og retningslinjer innen personellsikkerhet.

Det er viktig at personellsikkerhetsmessige tiltak settes i system for å oppnå best mulig effekt og tilstrekkelig kontroll på sikkerhetstilstanden.

Anbefaling til hvordan

- Få innlemmet i virksomhetens styringsdokument for sikkerhet at personellsikkerhet inngår i sikkerhetsstyringen.
- Få innlemmet ordlyd i virksomhetens personal og/eller tilsettingsreglement at vurdering av den best kvalifiserte til utlyste stillinger skal vurderes ut fra arbeidets innhold og sikkerhetsmessig egnethet.
- Utarbeid et O*verordnet dokument for personellsikkerhet*. Her kan mål og strategi for personellsikkerhet tydeliggjøres, sammen med fordeling av roller og ansvar for de ulike delene av arbeidet.
- Utarbeid en *Retningslinje for sikkerhet i rekruttering.* Her kan vurderingskriteriene for arbeidets innhold og sikkerhetsmessig egnethet fra Del 2 i denne veilederen bli utgangspunktet for underliggende rutiner.
- Utarbeid de underliggende rutinene for henholdsvis

➢ Nasjonal sikkerhet, med sikkerhetsklarering og autorisasjon

[18] Grunnprinsipper for personellsikkerhet .pdf

- Eksportkontroll og sanksjoner, med søknad og oppfølging av lisens
- Andre tungtveiende sikkerhetshensyn, med vurdering av sikkerhetsmessig egnethet og gjennomføring av bakgrunnssjekk.

- Sørg for at rutinene gir forutsigbarhet og likebehandling, gjennom å beskrive:
  - standardiserte vurderingskriterier som vil undersøkes
  - hvordan undersøkelsene gjennomføres
  - hvem som gjennomfører undersøkelsene
  - hvordan informasjonen som samles behandles

Utarbeid rutine for sikkerhet ved intern mobilitet
Denne må ivareta at sikkerhet vurderes etter de samme vurderingskritene som ved rekruttering, i saker der en ansatt skal gå over til annen stilling, eller også søker annen stilling internt i virksomheten, enten fast eller midlertidig.

Utarbeid rutine for gjesteforskere og andre tilknyttede
Den må ivareta at sikkerhet vurderes etter de samme kriterier som ved rekruttering.

Utarbeid rutiner for håndtering av hendelser og bekymring.
Denne rutinen må klargjøre hvor man kan si fra, og hvem som håndterer hva. Rutinen kan også inngå som tiltakskort i virksomhetens beredskapsplan.

Bruk Sikresiden

- Eksempel på styringsdokument for sikkerhet, hvor personellsikkerhet er definert inn sammen med de øvrige sikkerhetsområdene

- Eksempel på overordnet dokument for personellsikkerhet , med oversikt over forslag til underliggende retningslinjer og rutiner

DEL 4 REGELVERK, RISIKO OG VURDERINGSKRITERIER

Denne delen gir en oversikt over de mest aktuelle regelverkene som har betydning for arbeidet med personellsikkerhet, og som ligger til grunn for veilederens praktiske anbefalinger i del 1, 2 og 3.

Veilederen gir ikke en tolkning av regelverkene. Veilederen gir en enkel gjennomgang som har til hensikt å gi en grunnleggende oversikt over hva som er viktig å ta hensyn til ved sikkerhet i rekruttering og oppfølging, og hvilket handlingsrom for risikostyring virksomhetene har.

Det er viktig å være klar over at hver enkelt rekrutteringssak skal behandles individuelt og helhetlig. Det er i de aller fleste tilfeller rom for å vekte og vurdere de sammensatte forhold ulikt opp mot risiko og mulighet i den enkelte sak.

4.1 Universitets- og høyskoleloven

Universitets- og høyskoleloven[19] regulerer virksomheten ved universiteter og høyskoler i Norge. Loven gjelder for all høyere utdanning i Norge, inkludert utdanning som delvis foregår i utlandet, så lenge den har tilknytning til norsk virksomhet.

Kapittel 2 utdyper virksomhetenes ansvar for å sikre at undervisning, forskning og faglig eller kunstnerisk utviklingsarbeid holder et høyt faglig nivå, og at det utøves i tråd med anerkjente vitenskapelige, kunstneriske, pedagogiske og etiske prinsipper. Loven påpeker at virksomhetene skal samarbeide med relevante aktører både nasjonalt og internasjonalt. § 2-2 sier at universiteter og høgskoler skal fremme og verne akademisk frihet, og beskytte dem som utøver den. I *Retningslinjer og verktøy for ansvarlig internasjonalt kunnskapssamarbeid* omtaler HK-dir akademisk frihet og gir en oversikt over lovverk og internasjonale erklæringer som gjelder for ulike deler av kunnskapssektoren[20].

[19] Lov 8. mars 2024 nr. 9 om universiteter og høyskoler - https://lovdata.no/dokument/NL/lov/2024-03-08-9
[20] https://hkdir.no/retningslinjer-og-verktoy-for-ansvarlig-internasjonalt-kunnskapssamarbeid/akademiske-verdier-og-forskningsetikk/akademisk-frihet

Kapittel 7 omfatter ansettelser, og stiller krav om at virksomhetene aktivt skal arbeid for likestilling og hindre diskriminering. Det påpekes at undervisnings- og forskerstillinger som hovedregel skal lyses ut med kvalifikasjonskrav, og at innstilling av kandidater skal gjøres basert på disse kvalifikasjonskravene.

Universitets- og høgskoleloven lovfester ansvaret om å fremme og verne akademisk frihet og beskyttelse av dem som utøver den. Loven påpeker at virksomhetene skal samarbeide med relevante aktører både nasjonalt og internasjonalt. Loven skal fremme likestilling og hindre diskriminering. Arbeidet med personellsikkerhet må gjennomføres målrettet og balansert, slik at akademisk frihet og internasjonalt samarbeid kan utøves innenfor trygge rammer.

4.2 Statsansatteloven

Statsansatteloven[21] regulerer arbeidsforhold for arbeidstakere i staten, med regler for ansettelse, opphør av arbeidsforhold, ordenstraff og saksbehandling for ansatte i statlige virksomheter.

I § 3 redegjøres det for kvalifikasjonsprinsippet. Her fastsettes at den som vurderes som best kvalifisert for en stilling skal ansettes, med mindre det er gjort unntak i lov eller forskrift. Kvalifikasjonsprinsippet er tredelt, og gjelder:

- formell utdanning
- arbeidserfaring
- personlig egnethet

Kvalifikasjonskravene knyttet til disse tre forholdene skal vurderes i forkant, og beskrives i utlysningsteksten. Vurderingen av søkerne skal gjøres opp mot kvalifikasjonskravene i utlysningsteksten.

Det er i utgangspunktet opp til arbeidsgiver å bestemme hvilke kvalifikasjonskrav som er nødvendige og ønskelige for stillingen. Kvalifikasjonene arbeidsgiver setter som nødvendige eller ønskelige for stillingen må være innenfor alminnelige saklighetskrav. Det er også viktig å være kjent med de rettslige skrankene som følger av likestillings- og diskrimineringslovgivningen og personvernlovgivningen.

[21] Lov 16. juni 2017 nr. 67 om statens ansatte mv. - https://lovdata.no/dokument/NL/lov/2017-06-16-67

Statsansatteloven krever at kvalifikasjonsprinsippet overholdes, med mindre det det er unntak i lov eller forskrift. Når det er relevant for arbeidets innhold, kan det innenfor alminnelige saklighetskrav stilles krav til personlig sikkerhetsmessig egnethet, som del av kvalifikasjonskravet. Personlig sikkerhetsmessig egnethet må knyttes til forhold som arbeidsgiver kan undersøke.

4.3 Arbeidsmiljøloven

Arbeidsmiljøloven[22] regulerer grunnleggende forhold i norsk arbeidsliv, som arbeidsmiljø, stillingsvern, arbeidstid, permisjon, ansettelse og avslutning av arbeidsforholdet. Loven skal bidra til et inkluderende og helsefremmende arbeidsliv ved å sikre rettferdige arbeidsforhold og et fullt forsvarlig arbeidsmiljø.

I kapittel 4 stilles det krav til arbeidsmiljøet. § 4-3, første ledd sier at arbeidet skal organiseres, planlegges og gjennomføres slik at de psykososiale arbeidsmiljøfaktorene i virksomheten er fullt forsvarlige ut fra hensynet til arbeidstakernes helse, sikkerhet og velferd. § 4-3, tredje ledd sier at arbeidet skal legges til rette slik at arbeidstakers integritet og verdighet ivaretas.

Arbeidsmiljøloven påpeker også at arbeidsgivers plikter blant annet handler om å gi tilstrekkelig opplæring, sikre et forsvarlig arbeidsmiljø, og utøve sin omsorgsplikt. Videre peker den på at arbeidstakers plikter blant annet handler om å innordne seg arbeidsgivers styringsrett, ta til seg opplæring, medvirke og opptre lojalt.

Stillingsvernsreglene i kapittel 15 og reglene om kontrolltiltak i kapittel 9, er sentrale reguleringer i arbeidet med personellsikkerhet. Kontrolltiltak som besluttes må ha en saklig grunn, ikke være uforholdsmessige og må evalueres med tillitsvalgte før de besluttes. Hovedavtalen i staten beskriver blant annet hvordan slik medbestemmelse skal gjennomføres[23].

[22] Lov 17. juni 2005 nr. 62 om arbeidsmiljø, arbeidstid og stillingsvern mv. - https://lovdata.no/dokument/NL/lov/2005-06-17-62
[23] https://www.regjeringen.no/no/dokumenter/hovedavtalen-i-staten/id2952431/?ch=1

Arbeidsmiljøloven ivaretar grunnleggende rettigheter som rettferdige arbeidsforhold og krav til at faktorene i arbeidsmiljøet er fullt forsvarlige ut fra hensynet til helse, miljø og sikkerhet. Arbeidet med personellsikkerhet må gjennomføres i tråd med disse kravene, slik at den enkeltes integritet, verdighet og grunnleggende rettigheter ivaretas, i et fullt forsvarlig arbeidsmiljø. Medvirkning, god kommunikasjon og målrettet opplæring vil være viktig for å oppnå dette.

4.4 Personopplysningsloven

Personopplysningsloven[24] regulerer behandling av personopplysninger. Lovens formål er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Behandlingen av personopplysninger må ha et klart definert og lovlig formål og det skal ikke behandles mer personopplysninger enn nødvendig. De registrerte skal ha mottatt tilstrekkelig informasjon om den aktuelle behandlingen.

Opplysninger om blant annet etnisk opprinnelse, helseopplysninger og religion er definert som særlige kategorier av personopplysninger (sensitive personopplysninger) og er i utgangspunktet forbudt å behandle. GDPR art. 9 nr. 2 åpner likevel for behandling av slike opplysninger hvis nærmere vilkår er oppfylt.

Artikkel 9 nr. 2 bokstav b åpner for å behandle slike særlige kategorier av personopplysninger hvis det er tale om å oppfylle forpliktelser eller utøve rettigheter på området arbeidsrett, forutsatt at forholdet er regulert i lov eller tariffavtale. Personopplysningsloven § 6 gir hjemmel til å behandle særlige kategorier av personopplysninger i arbeidsforhold.

All behandling av personopplysninger forutsetter et behandlingsgrunnlag i art. 6 nr. 1. De aktuelle grunnlagene i forbindelse med personellsikkerhet vil være bokstav b. om avtaleinngåelse eller avtaleoppfyllelse, bokstav c. om rettslig forpliktelse der det foreligger, eventuelt bokstav f. om arbeidsgivers berettigede interesse. Arbeidsgiver vil ha en berettiget interesse av informasjon om person som kan ha betydning for virksomhetens sikkerhetsstyring. I noen tilfeller er samtykke tilstrekkelig, f.eks. der man ønsker å verifisere

[24] Lov 15. juni 2018 nr. 38 om behandling av personopplysninger - https://lovdata.no/dokument/NL/lov/2018-06-15-38

at oppgitte tidligere stillinger, arbeidsgivere og utdanningsgrader er korrekt. Man må altså ikke alltid ha hjemmel/pålegg i lov som bokstav c gjelder.

Samtykke er et noe usikkert rettslig grunnlag å basere behandlingen av personopplysninger på i forbindelse med rekrutteringsprosesser. Selv om det kan være ryddig å be om samtykke til å innhente informasjon i rekrutteringsprosesser, kan skjevheten i maktforholdet mellom arbeidsgiver og -søker eller -taker tilsi at et slikt samtykke ikke er helt frivillig avgitt.

Personopplysingsloven lovfester ansvaret om å beskytte enkeltpersonens personopplysninger, og sikre at disse behandles ut fra et lovmessig forankret grunnlag på en rettferdig og transparent måte. Reglene som gjelder behandling av personopplysninger er også viktig i arbeidet med personellsikkerhet, i rekrutteringsprosesser og i forvaltningen av arbeidsforhold.

4.5 Likestillings- og diskrimineringsloven

Likestillings- og diskrimineringsloven (ldl)[25] formål er å fremme likestilling og hindre diskriminering. Likestillings- og diskrimineringsombudet (LDO) har utarbeidet en veiledning om sikkerhetsvurderinger i arbeidsforhold[26], som blant annet sier følgende:

«Ldl § 6 forbyr diskriminering. Diskriminering er definert som forskjellsbehandling som knytter seg til et eller flere diskrimineringsgrunnlag som er listet opp i ldl. § 6 første ledd. Etnisitet er ett av flere vernede grunnlag som loven lister opp. Loven definerer etnisitet som blant annet *nasjonal opprinnelse, avstamning, hudfarge og språk*. Diskrimineringsforbudet omfatter diskriminering på grunn av eksisterende, antatte, tidligere eller fremtidige forhold. Det følger av ldl. § 6 tredje ledd at forbudet også gjelder hvis en person blir diskriminert på grunn av sin tilknytning til en annen person og diskrimineringen er knyttet til denne personens etnisitet. Det vil si at det for eksempel kan være diskriminering å legge vekt på etnisiteten til arbeidssøkerens kjæreste eller samboer, eller kjærestens/samboerens tilknytning til andre land.

[25] Lov 16. juni 2017 nr. 51 om likestilling og forbud mot diskriminering - https://lovdata.no/dokument/NL/lov/2017-06-16-51
[26] Se Vedlegg x hele brevet

Selv om forskjellsbehandling på grunn av etnisitet som hovedregel er forbudt, kan det være lovlig hvis vilkårene for lovlig forskjellsbehandling i ldl. § 9 er oppfylt. I arbeidsforhold er det en skjerpet adgang til å forskjellsbehandle på grunn av etnisitet – det er kun tillatt med direkte forskjellsbehandling på grunn av etnisitet hvis etnisiteten har avgjørende betydning for utøvelsen av arbeidet eller yrket. I tillegg må forskjellsbehandlingen være nødvendig for å oppnå et saklig formål og forholdsmessig overfor den som forskjellsbehandles.

Ifølge ldl. § 29 gjelder diskrimineringsforbudet alle sider av et arbeidsforhold, blant annet ved utlysning av stilling, ansettelse, omplassering, forfremmelse og opphør av arbeidsforholdet. Ldl. § 30 innebærer et forbud mot å innhente visse opplysninger i ansettelsesprosesser, blant annet opplysninger om en søkers etnisitet. Dette gjelder ikke dersom opplysningene har avgjørende betydning for utøvelsen av arbeidet eller yrket. Ldl. § 30 gjelder også innhenting av opplysninger om tredjepersoner som en arbeidssøker har tilknytning til, se for eksempel sak i Diskrimineringsnemda 22/1093[27]»

Diskrimineringsnemda[28] er et nøytralt, statlig organ som avgjør saker om diskriminering, trakassering, seksuell trakassering og gjengjeldelse. Vedtak fra reelle saker av nyere tid vedrørende forskjellsbehandling på grunn av vernede grunnlag, viser hvordan alle fire vilkår i § 9 må være oppfylt for at en forskjellsbehandling skal være lovlig. I flere saker vedrørende *etnisitet* er *tungtveiende sikkerhetshensyn* lagt til grunn i i vilkårene.

Likestillings- og diskrimineringsloven oppstiller et viktig vern mot å bli diskriminert. Arbeidet med personellsikkerhet må gjennomføres slik at en eventuell forskjellsbehandling på grunn av vernede grunnlag, som eksempelvis etnisitet, oppfyller samtlige vilkår i i § 9, og er godt og saklig dokumentert.

4.6 Sikkerhetsloven med tilhørende forskrifter

De statlig eide universitetene og høgskolene er underlagt sikkerhetsloven[29]. I *Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor*[30] beskriver KD hvordan virksomhetene skal imøtekomme kravene til nasjonal sikkerhet.

[27] 22-1093-offentlig-versjon-av-uttalelse.pdf
[28] https://www.diskrimineringsnemnda.no/
[29] Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet - https://lovdata.no/dokument/NL/lov/2018-06-01-24
[30] Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor

4.6.1 Sikkerhetsloven

Loven skal bidra til å trygge *Norges nasjonale sikkerhetsinteresser* (NSI), som i loven er definert som landets suverenitet, territorielle integritet og demokratiske styreform, og overordnede sikkerhetspolitiske interesser knyttet til

- de øverste statsorganers virksomhet, sikkerhet og handlefrihet
- forsvar, sikkerhet og beredskap
- forholdet til andre stater og internasjonale organisasjoner
- økonomisk stabilitet og handlefrihet
- samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet

Disse nasjonale sikkerhetsinteressene understøttes igjen av det som i sikkerhetsloven § 1-5 nr. 2 omtales som *grunnleggende nasjonale funksjoner* (GNF). GNF er definert som tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.

Loven benytter begrepet *skjermingsverdig* om verdier som skal beskyttes etter lovens bestemmelser. Slike verdier er spesifisert som *informasjon, informasjonssystemer, objekter og infrastruktur*. De vil være skjermingsverdige fordi de enten støtter opp om de grunnleggende nasjonale funksjonene, eller ved at de i seg selv har betydning for nasjonale sikkerhetsinteresser.

Bestemmelsene i sikkerhetsloven med forskrift skal bidra til å forebygge, avdekke og motvirke sikkerhetstruende virksomhet som kan påvirke disse verdiene. Loven poengterer i formålsparagrafen at sikkerhetstiltak skal gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

4.6.2 Virksomhetsikkerhetsforskriften[31]

Virksomhetssikkerhetsforskriften kapittel 2 stiller krav om at virksomheter som er underlagt sikkerhetsloven skal ha sikkerhetsstyring. Videre presiserer forskriften gjennomgående hvilke konkrete krav som gjelder for å beskytte skjermingsverdig informasjon, informasjonssystemer, objekter og infrastruktur.

[31] Forskrift 20. desember 2018 nr. 2053 om virksomheters arbeid med forebyggende sikkerhet - https://lovdata.no/dokument/SF/forskrift/2018-12-20-2053

4.6.3 Forskrift om sikkerhetsklarering og annen klarering[32]

Klareringsforskriften presiserer bestemmelsene i sikkerhetsloven om ansvar og prosesser for sikkerhetsklaring, adgangsklarering og personkontroll, og for informasjonsinnhenting, -utlevering og -behandling i den forbindelse.

Det er Nasjonal sikkerhetsmyndighet (NSM) som, på vegne av Justisdepartementet og Forsvarsdepartementet, er tilsynsmyndighet og fagmyndighet innenfor forebyggende sikkerhet i henhold til sikkerhetsloven med forskrift[33]. NSM har en rekke håndbøker og veiledere for hvordan vurdere verdier og håndtere risiko innenfor nasjonal sikkerhet.

4.6.4 Om skjermingsverdige verdier

Informasjon er skjermingsverdig hvis det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig, jf. sikkerhetsloven § 5-1.

Et informasjonssystem er skjermingsverdig hvis det behandler skjermingsverdig informasjon, eller hvis det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner eller for nasjonale sikkerhetsinteresser, jf. sikkerhetsloven § 6-1.
Objekter og infrastruktur er skjermingsverdige hvis de kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet, blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse, eller kan skade nasjonale sikkerhetsinteresser på annen måte, jf. sikkerhetsloven § 7-1.

Kunnskapsdepartementet skal innenfor sitt ansvarsområde utpeke, klassifisere og holde oversikt over *skjermingsverdige objekter og infrastruktur*[34]. Det følger av sikkerhetsloven § 2-1 at departementene er ansvarlig for forebyggende sikkerhetsarbeid innenfor sitt ansvarsområde.

4.6.5 Om sikkerhetsgradert informasjon

Det er viktig å være klar over begrepene «ugradert skjermingsverdig informasjon» og «sikkerhetsgradert informasjon».

[32] https://lovdata.no/dokument/SF/forskrift/2018-12-20-2054
[33] instruks-for-nsm.pdf
[34] https://www.regjeringen.no/contentassets/f856bbb85cf9499cb5fbfb74110b23bc/no/pdfs/styringsdokument_sikkerhet-og-beredskap.pdf

- *Ugradert skjermingsverdig informasjon* brukes i virksomhetssikkerhetsforskriften § 22 om informasjon med skadepotensial for nasjonal sikkerhet knyttet til om den blir endret eller blir utilgjengelig, altså *integritet og tilgjengelighet*.

- *Sikkerhetsgradert informasjon* betyr at det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, og informasjonen må derfor beskyttes som følge av behov for *konfidensialitet,* jf. sikkerhetsloven § 5-3.

Sikkerhetsloven § 5-3 sier at 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:

- STRENGT HEMMELIG dersom det kan få helt avgjørende skadefølger
- HEMMELIG dersom det kan få alvorlige skadefølger
- KONFIDENSIELT dersom det kan få skadefølger
- BEGRENSET dersom det i noen grad kan få skadefølger.

Andre ledd i bestemmelsen sier at sikkerhetsgradering ikke skal brukes i større utstrekning eller for lengre tid enn nødvendig. Sikkerhetsloven § 5-4 sier at sikkerhetsgradert informasjon skal bare overlates til personer som har tjenstlig behov og er autorisert for tilgang til slik informasjon.

NSM har en veileder i sikkerhetsgradert informasjon[35].

4.6.6 Nasjonal sikkerhet og personellsikkerhet

Kapittel 8 i sikkerhetsloven beskriver krav til personellsikkerhet. § 8-1 sier at personer som skal få tilgang til *sikkerhetsgradert informasjon*, eller som skal ha adgang til *skjermingsverdige objekter og infrastruktur*, skal autoriseres. Hvis de skal autoriseres for tilgang til informasjon gradert KONFIDENSIELT eller høyere, må de i tillegg ha gyldig sikkerhetsklarering. Personer som skal autoriseres for adgang til skjermingsverdige objekter og infrastruktur må ha gyldig adgangsklarering.

[35] https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker/veileder-i-sikkerhetsgradert-informasjon

I kapittel 12 i virksomhetssikkerhetsforskriften er det beskrevet krav om klarering og autorisasjon.

Sikkerhetslovens § 8-4 om avgjørelse om klarering, sier at i vurderingen av om hvorvidt en person er sikkerhetsmessig skikket, så skal det legges vekt på forhold som er relevante for personens *pålitelighet, lojalitet og dømmekraft* i forbindelse med behandling av gradert informasjon og tilgang til skjermingsverdige objekter og infrastruktur.

§ 8-2 sier at også personer som gjennom sitt arbeid *vil kunne få tilgang* til informasjon gradert KONFIDENSIELT eller høyere, skal sikkerhetsklareres. Samtidig understrekes det i andre ledd at sikkerhetsklarering likevel ikke skal gjennomføres dersom risikoen for tilgang til slik informasjon kan fjernes gjennom andre og enklere sikkerhetstiltak.

Klareringsforskriftens § 16[36] sier at den som er sikkerhetsklarert for KONFIDENSIELT eller høyere er også klarert for adgang til skjermingsverdige objekt eller infrastruktur med krav om adgangsklarering.
Sikkerhetsklarering og autorisasjon skal følge *tjenstlig behov*[37], og skal ikke brukes med mindre det er nødvendig for å beskytte skjermingsverdige verdier.

4.6.7 Om klarering og autorisasjon av utenlandsk person

Sikkerhetslovens § 8-7[38] sier at klarering av personer med utenlandsk statsborgerskap kan, etter en konkret helhetsvurdering få klarering, dersom det ikke er rimelig grunn til å tvile på at personen er sikkerhetsmessig skikket. I tillegg til forholdene i § 8-4 skal det i vurderingen legges vekt på *hjemlandets sikkerhetsmessige betydning, personens tilknytning og tilknytningen til Norge*.

Klareringsforskriftens § 18[39] sier i 1. og 2. ledd at Nasjonal sikkerhetsmyndighet skal utarbeide sikkerhetsmessige vurderinger av relevante staters betydning for norske sikkerhetsinteresser i klareringssaker. Klareringsmyndigheten skal legge vekt på vurderingene i saker der personer som inngår i personkontrollen har tilknytning til andre stater.

[36] https://lovdata.no/forskrift/2018-12-20-2054/§16
[37] https://nsm.no/getfile.php/132407-1590749199/NSM/Filer/Dokumenter/Veiledere/Veileder%20i%20personellsikkerhet.pdf
[38] https://lovdata.no/lov/2018-06-01-24/§8-7
[39] https://lovdata.no/forskrift/2018-12-20-2054/§18

Virksomhetssikkerhetsforskriftens § 70 1. og 2. ledd[40] sier at før en utenlandsk statsborger som ikke har klarering, kan autoriseres for informasjon gradert BEGRENSET, skal den autorisasjonsansvarlige vurdere om *personens tilknytning til hjemlandet og hjemlandets sikkerhetsmessige betydning utgjør en uakseptabel risiko*. Den autorisasjonsansvarlige kan be klareringsmyndigheten om en vurdering av hjemlandets sikkerhetsmessige betydning. Dersom en utenlandsk statsborger kommer fra en stat som Politiets sikkerhetstjeneste mener utgjør en høy sikkerhetsrisiko for Norge, må den autorisasjonsansvarlige innhente samtykke fra en klareringsmyndighet før den utenlandske statsborgeren kan autoriseres for BEGRENSET.

Klareringsforskriftens § 13[41] om vurdering av personkontrollopplysninger sier i 3. ledd at for at en personkontroll skal kunne brukes i en klarering av en person som har oppholdt seg i utlandet, må Norge ha et sikkerhetssamarbeid med oppholdsstatene som gjør det mulig for Nasjonal sikkerhetsmyndighet å innhente registeropplysningene angitt i § 8 og § 9 fra disse statenes myndigheter. Dersom Nasjonal sikkerhetsmyndighet ikke kan innhente registeropplysninger fra en annen stat, skal klareringsmyndigheten vurdere om opplysningene som stammer fra andre kilder, og som er mulig å verifisere på en enkel måte, kan kompensere for manglende eller ufullstendige registeropplysninger.

4.6.8 Nasjonal sikkerhet i UH-sektoren

For virksomhetene underlagt KD gjelder rutinene som er beskrevet i kapittelet om *Krav og forventninger til virksomhetenes arbeid med nasjonal sikkerhet*, i Styringsdokument for arbeid med sikkerhet og beredskap i Kunnskapsdepartementets sektor[42]. Klareringssak gjennomføres ved at virksomheten ved behov for sikkerhetsklarering, oversender søknad med begrunnelse til KD. Departementet anmoder klareringsmyndigheten, som for den sivile UH-sektoren vil være Sivil klareringsmyndighet[43], om klarering av personen. Virksomheten selv gjennomfører autorisasjonen.

Vurderinger av hvorvidt verdier bør være skjermingsverdige etter sikkerhetsloven er et pågående modnings- og utviklingsarbeid i UH-sektoren. KD har gjennom sine vurderinger så langt identifisert to områder som *grunnleggende nasjonale funksjoner* innenfor eget ansvarsområde[44]:

[40] https://lovdata.no/forskrift/2018-12-20-2053/§70
[41] https://lovdata.no/forskrift/2018-12-20-2054/§13
[42] https://www.regjeringen.no/contentassets/f856bbb85cf9499cb5fbfb74110b23bc/no/pdfs/styringsdokument_sikkerhet-og-beredskap.pdf
[43] Klarering – Sivil klareringsmyndighet
[44] Oversikt over innmeldte grunnleggende nasjonale funksjoner - Nasjonal sikkerhetsmyndighet

- Kunnskapsdepartementets virksomhet, handlefrihet og beslutningsdyktighet
- Forskning og utvikling av betydning for nasjonal sikkerhet

KD har stilt krav gjennom årlige tildelingsbrev at de underlagte virksomhetene skal vurdere hvilke verdier de har som er av betydning for nasjonale sikkerhetsinteresser, og som skal anses og behandles som *skjermingsverdige*. Dette kan handle om objekter, infrastruktur, informasjon og informasjonssystemer.

Virksomheter kan eksempelvis gjennom forskningssamarbeid med eksterne partnere behandle sikkerhetsgradert informasjon eller gis adgang til skjermingsverdige objekter eller infrastruktur. I slike sammenhenger er det nødvendig med avklaring av ansvar for nødvendige klareringer og autorisasjon, og for hvordan oppfølging skal gjennomføres.

NSM er fagmyndighet for personellsikkerhet innenfor sikkerhetslovens virkeområde og har veiledere og håndbøker som omhandler personellsikkerhet:

4.6.9 NSMs Veileder i personellsikkerhet[45]:

Denne veilederen omhandler bestemmelsene om personellsikkerhet i sikkerhetsloven kapittel 8 og forskrift om virksomheters arbeid med forebyggende sikkerhet og forskrift om sikkerhetsklarering og annen klarering. Veilederen gir uttrykk for hvordan bestemmelsene om personellsikkerhet skal forstås.

4.6.10 NSMs Håndbok i autorisasjon[46]:

Målgruppen for håndbok i autorisasjon er personer som skal autorisere personell for tilgang til sikkerhetsgradert informasjon, eller skjermingsverdig objekt, system eller infrastruktur. Den kan også være til nytte for den som skal autoriseres for å få kunnskap om hva de kan forvente av autorisasjonsansvarlige, og hva autorisasjon innebærer.

Sikkerhetsloven med forskrifter har til hensikt å beskytte verdier med betydning for nasjonale sikkerhetsinteresser. Universiteter og høgskoler som har *sikkerhetsgradert informasjon* eller *skjermingsverdige objekter og infrastruktur,* eller som har samarbeid med aktører som innbefatter behandling av slike verdier, må følge de personellmessige

[45] https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker/veileder-i-personellsikkerhet/om-denne-veilederen/
[46] https://nsm.no/getfile.php/1314578-1743622116/NSM/Filer/Dokumenter/Veiledere/H%C3%A5ndbok%20i%20autorisasjon.PDF

kravene knyttet til klarering og autorisasjon. Disse kravene skal følge av et tjenstlig behov.

Klarering og autorisasjon handler om å undersøke forhold som har betydning for en persons sikkerhetsmessige skikkethet. Dette er presisert som personens pålitelighet, lojalitet og dømmekraft.

Det er Sivil klareringsmyndighet som gjennomfører personkontrollen i klareringssaker. Autorisasjon gjennomføres av virksomheten selv.

Klarering og autorisasjon av personer med utenlandske statsborgerskap er presisert i lov og forskrifter at gjennomføres av klareringsmyndigheten i en helhetlig vurdering i den enkelte sak, hvor klareringsmyndigheten vil vektlegge hjemlandets sikkerhetsmessige betydning, personens tilknytning og tilknytningen til Norge.

Loven poengterer i formålsparagrafen at sikkerhetstiltak skal gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

4.7 Eksportkontroll- og sanksjonsregelverket

Eksportkontrollregelverket består av eksportkontrollloven, eksportkontrollforskriften, og Retningslinjer for Utenriksdepartementets behandling av søknader om eksport av forsvarsmateriell, samt teknologi og tjenester for militære formål av 28. februar 1992[47]. I tillegg er flere sanksjonsforskrifter relevante. Både eksportkontroll og sanksjoner er tett koblet til nasjonal sikkerhet.

Eksportkontroll innebærer at visse varer, teknologi og tjenester ikke kan eksporteres fra Norge uten lisens utstedt av myndighetene[48]. Dette er varer, teknologi og tjenester som kan påvirke militære styrkeforhold, og som er en viktig del av norsk sikkerhetspolitikk. Innenfor kunnskapssektoren handler eksportkontroll hovedsakelig om kontroll med teknologioverføring, som ved forskningssamarbeid[49].

---

47 https://www.regjeringen.no/globalassets/departementene/ud/vedlegg/eksportkontroll/eksportkontroll_retningslinjer190506.pdf

48 Eksportkontroll - regjeringen.no

49 https://www.regjeringen.no/contentassets/ca0e63363cc54c448928ed14e6726445/veileder-for-eksport-av-teknologi-august-2025-utenriksdepartementet.pdf

4.7.1 Eksportkontrolloven[50]

Etter eksportkontrolloven § 1 skal 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, ikke utføres fra Norge uten særskilt tillatelse (lisens). Loven er kortfattet, og forskriftshjemmelen er brukt til å fastsette eksportkontrollforskriften.

4.7.2 Eksportkontrollforskriften[51]

Denne beskriver nærmere hvilke angitte varer, teknologi, samt visse tjenester som er kontrollert, det vil si at disse ikke kan eksporteres eller overføres ut av landet uten lisens. Forskriften omhandler også hvilke plikter og bestemmelser som gjelder ved eksport.
De angitte varene som er relevante for universiteter og høgskoler er i forskriften omtalt som *flerbruksvarer* og er oppført i vareliste II og III til eksportkontrollforskriften, jf. § 2 andre ledd.

§ 2 gir også øvrige definisjoner på hva som menes med eksport, overføring, leverandør, mottaker, lisens, overføringslisens, transitt og teknologi. I det10. ledd er teknologi definert slik: «Med teknologi som oppført i vedlegg I, II og III til denne forskrift menes spesifikk informasjon nødvendig for utvikling, produksjon eller bruk av varer. Slik informasjon vil være tekniske data eller bistand. I § 7 omfatter teknologi i tillegg enhver annen teknisk data og teknisk bistand.»

4.7.3 Sanksjonsloven[52] med sanksjonsforskrifter

Sanksjonsloven § 2 sier at Norge kan gjennomføre sanksjoner eller restriktive tiltak som er vedtatt i mellomstatlige organisasjoner, eller som ellers har bred internasjonal oppslutning, og som har som formål å opprettholde fred og sikkerhet eller sikre respekt for demokrati og rettsstat, menneskerettigheter eller folkeretten for øvrig[53]. Norge er folkerettslig forpliktet til å gjennomføre geografiske og tematiske sanksjonsregimer vedtatt av FNs sikkerhetsråd og EU[54].

[50] Lov 18. desember 1987 nr. 93 om kontroll med eksport av strategiske varer, tjenester og teknologi m.v. - https://lovdata.no/dokument/NL/lov/1987-12-18-93
[51] Forskrift 19. juni 2013 nr. 718 om eksport av forsvarsmateriell, flerbruksvarer, teknologi og tjenester - https://lovdata.no/dokument/SF/forskrift/2013-06-19-718
[52] https://lovdata.no/dokument/NL/lov/2021-04-16-18
[53] https://lovdata.no/lov/2021-04-16-18/§2
[54] Gjeldende sanksjoner – DEKSA

Utenriksdepartementet (UD) er myndighet på eksportkontroll og sanksjoner i Norge. Direktoratet for eksportkontroll og sanksjoner (DEKSA) er den nasjonale fagmyndigheten for eksportkontroll og sanksjoner, og behandler søknader om eksportlisens[55].
UD har utarbeidet en *Veileder for eksport av teknologi*[56] som berørte virksomheter og aktuelle fagmiljøer må sette seg inn i, og som denne veilederen i hovedsak tar utgangspunkt i det videre.

4.7.4 Om lisenspliktig teknologi

På sidene 11-12 i *Veileder for eksport av teknologi* presiseres hva som menes med lisenspliktig teknologi:

«Teknologi i denne sammenheng er definert i forskriften § 2 (10), men fastsetter ikke hva som er lisenspliktig. For at informasjon skal regnes som teknologi må den være spesifikk, nødvendig og teknisk, som definert i vedleggene (varelistene) til forskriften. Dette er et grunnvilkår for at informasjon i det hele tatt skal være gjenstand for vurdering etter regelverket. Den som skal overføre teknologi må selv vurdere innholdet i listene for å identifisere om det er lisensplikt for teknologien og hvilken klassifisering som er riktig. Vurderingen kan også føre til konklusjon om at teknologien ikke er lisenspliktig. Etter varelistene er det selve teknologien som utløser lisensplikten, ikke konteksten den inngår i, eksempelvis hvilken funksjon den er oppfunnet for eller hva den skal brukes til. Dette skiller lisensplikt etter varelistene fra § 7 ("fang-alt"), hvor konteksten er en sentral vurdering.

For at informasjon skal omfattes av kontrollen med teknologi, må den være spesifikk for utvikling, produksjon eller bruk av en listeført vare. Det er ikke tilstrekkelig at informasjonen har en løs tilknytning til slike prosesser. Informasjonen må være nødvendig for å kunne oppnå eller forbedre de kontrollerte ytelsesnivåene, egenskapene eller funksjonene til varen.»

På side 20 presiseres hva som menes med «fang-alt»-bestemmelsene:

«Hovedtrekkene ved «fang-alt»-bestemmelser er at de gir myndighetene hjemmel til å ilegge enhver vare, teknologi eller tjeneste lisensplikt under nærmere angitte omstendigheter. Norge har fire «fang-alt»- bestemmelser i forskriften § 7 bokstavene a-d,

[55] Hva er eksportkontroll? - regjeringen.no
[56] https://www.regjeringen.no/contentassets/ca0e63363cc54c448928ed14e6726445/veileder-for-eksport-av-teknologi-august-2025-utenriksdepartementet.pdf

samt i § 5 om lisensplikt for tjenester. Formålet med «fang-alt» avhenger av hvilken av de fire reglene man anvender. Virkeområdet er snevert, som betyr at det er høy terskel for myndighetene å ta i bruk mulighetene for slik kontroll, og en slik sak skal være koblet til nasjonale sikkerhetshensyn.»

Unntak fra lisensplikt er beskrevet i kapittel 6 i UDs veileder.

4.7.5 Eksportkontrollregelverket, sanksjoner og personellsikkerhet

DEKSA[57] er nasjonal fagmyndighet på området og behandler søknader om lisens. For den sivile kunnskapssektoren vil vareliste II og nasjonal vareliste III være relevante[58]. DEKSA påpeker at sanksjonsforskrifter også kan gjelde i tillegg til eksportkontrollregelverket, når berørte personer kommer fra sanksjonerte land.

DEKSA poengterer at en *lisenspliktig teknologioverføring* til en utenlandsk statsborger som befinner seg i Norge anses som en eksport til landet den aktuelle mottakeren er statsborger av. I internasjonal sammenheng omtales dette som «deemed exports», altså at eksport til utenlandske statsborgere anses som en eksport til personens hjemland, uavhengig av om teknologien rent fysisk forlater landet eller ei.

Universitetene og høgskolene må vurdere om forskningen og teknologien de utvikler har spesifikasjoner som er på varelistene, og hvordan de må etterkomme de regelverkskravene som medfølger. DEKSA påpeker i sine retningslinjer[59] at utdanningsinstitusjonenes opptak av utenlandske studenter og ansettelser av utenlandske personer til sensitive fagområder krever særlig årvåkenhet og aktsomhet.

Utdanningsinstitusjonene må selv vurdere sensitiviteten i fagområdene og emnene som tilbys ved deres institusjon og samtidig vurdere hvorvidt overføring av slik kunnskap til den enkelte student, stipendiat eller ansatte vil være i strid med norsk eksportkontrollregelverk.

Utdanningsinstitusjonene må også være oppmerksomme på at eksportkontrollregelverket kommer til anvendelse ved forskningssamarbeid og deling av informasjon og

[57] DEKSA
[58] https://www.regjeringen.no/contentassets/ca0e63363cc54c448928ed14e6726445/veileder-for-eksport-av-teknologi-august-2025-utenriksdepartementet.pdf
[59] https://deksa.no/eksportkontroll/trenger-du-lisens/kunnskapsoverforing/

forskningsresultater med utenlandske institusjoner, samt ved annen tilgjengeliggjøring av slik informasjon og ved deltagelse eller gjennomføring av kurs og konferanser.

Regelverket fordrer at hver enkelt studie- og arbeidssøknad behandles individuelt.

Eksportkontrollregelverket har betydning for universiteter og høgskoler ved rekruttering og oppfølging av vitenskapelig personell innenfor fag- og teknologiområder som kan innebære tilgang til eller utvikling av flerbruksvarer og teknologi som er regulert av regelverket.

Den som ansettes, eller den som skal jobbe med slike regulerte verdier må innvilges nødvendig lisens dersom vedkommende har utenlandsk statsborgerskap og ikke kommer inn under unntakene for lisensplikt. Personlig sikkerhetsmessig egnethet vil være nødvendig å vurdere, og må knyttes til forhold som arbeidsgiver kan undersøke.

Det er DEKSA som behandler søknader om lisens. Hver søknad behandles individuelt.

4.8 Samfunnsviktige tjenester eller tilbydere av digitale tjenester (NIS1- og 2)

Digitalsikkerhetsloven med forskrift er innlemming av krav fra (EU) 2016/1148 (NIS-direktivet) i norsk rett. NSM har utarbeidet en egen veileder for virksomhetene som treffes av regelverket [60]. I NIS2-direktivet som ble vedtatt i EU i 2022, *identifiseres offentlig forvaltning som kritisk for samfunnet*, og *forskning som særlig viktig for samfunnet*. NIS2-direktivet vil også etter hvert innlemmes i norsk lov og erstatte NIS1-direktivet.

4.8.1 Digitalsikkerhetsloven

Digitalsikkerhetsloven[61] skal bidra til å sikre grunnleggende krav til digital sikkerhet i virksomheter med særlig betydning for samfunnet. Denne loven treffer de som tilbyr såkalte *samfunnsviktige tjenester*, og de som er tilbydere av *digitale tjenester*.

[60] Veileder fra NSM i digitalsikkerhetsloven og -forskriften.pdf
[61] Lov 20. desember 2023 nr. 108 om digital sikkerhet - https://lovdata.no/dokument/NL/lov/2023-12-20-108

I § 2 blir tilbydere av samfunnsviktige tjenester spesifisert som *energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur* og *digital infrastruktur*. Videre utdypning er listet opp i digitalsikkerhetsforskriften[62] § 1.

Dette er virksomheter som leverer tjenester som er viktig for å opprettholde kritiske samfunnsmessige eller økonomiske aktiviteter. Disse er avhengige av nettverks- og informasjonssystemer for å levere tjenesten, og kan få tjenesteleveransen betydelig forstyrret av en hendelse.

Tilbydere av digitale tjenester som omfattes av digitalsikkerhetsloven er spesifisert i § 9. Dette er virksomheter som tilbyr tjenester i form av nettbaserte markedsplasser, nettbaserte søkemotorer eller skytjenester, som definert i ehandelsloven[63] § 1.

4.8.2 Digitalsikkerhetsforskriften

I kapittel 2 spesifiseres kravene til tilbydere av slike tjenester. Det stilles krav til styringssystem for sikkerhet, risikovurderinger og risikohåndtering, organisatoriske, teknologiske, personellmessige og fysiske sikkerhetstiltak, og for hendelseshåndtering og beredskap.

I § 12 stilles det særlige krav til personellmessige sikkerhetstiltak. Adgang til lokaler og tilganger til nettverk og informasjonssystemer skal tildeles basert på roller, oppgaver, ansvar og tjenstlig behov, og det skal følges opp at personell ikke har flere tilganger enn nødvendig. Ansatte, leverandører og oppdragstakere som kan få tilgang til virksomhetens nettverk og informasjonssystemer skal gjøres kjent med relevante sikkerhetstiltak, slik at de har tilstrekkelig kompetanse innenfor sikkerhet og de skal gis nødvendig opplæring ved behov.

4.8.3 Forskrift om sikkerhet og beredskap i kraftforsyningen

Kraftberedskapsforskriften følger opp om energilovens § 1-2 og skal sikre at kraftforsyningen opprettholdes, og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene. Denne forskriften gjelder for alle såkalte KBO-enheter, som i § 2-1 er nærmere definert.

[62] Forskrift 20. juni 2025 nr. 1131 om digital sikkerhet - https://lovdata.no/forskrift/2025-06-20-1131/
[63] Lov 23. mai 2003 nr. 35 om visse sider av elektronisk handel og andre informasjonssamfunnstjenester - https://lovdata.no/lov/2003-05-23-35/

I § 6-7, 1. og 2. ledd om personkontroll står det at KBO-enheter skal gjennomføre en bakgrunnssjekk av personer før ansettelse, og at personer i spesifiserte tilfeller skal fremlegge kredittsjekk. I 4. ledd står det at disse undersøkelsene skal brukes som grunnlag for å vurdere en persons egnethet til å få tilgang til klassifiserte anlegg, systemer eller annet.

4.8.4 Samfunnsviktige tjenester og personellsikkerhet

I *Veileder fra NSM i digitalsikkerhetsloven og -forskriften* utdypes nærmere hva som kan inngå i slike nettverks- og informasjonssystemer, og hva tilbydere er forpliktet til å gjøre for å holde et forsvarlig sikkerhetsnivå[64]. Veilederen sier i punkt 6.2.5 at sikkerhetstiltakene skal være

- «proporsjonale»; som innebærer vurdering av kostnad og nytte, og
- «hensiktsmessige»; som innebærer at tiltakene må være egnet for å bidra til forsvarlig sikkerhet.

Dette gjelder også for tiltak som omhandler personellsikkerhet i punkt 6.2.8, og som vil omhandle ansatte, leverandører og oppdragstakere som får tilgang til nettverks- og informasjonssystemene. En tilbyder av slike tjenester må kunne vurdere at personen er pålitelig, og kan stille krav til personlig sikkerhetsmessig egnethet for å gjøre slike vurderinger.

Norges Vassdrags- og energidirektorat (NVE) har i egen *Veiledning til kraftberedskapsforskriften*[65] presisert hva som menes med personkontroll etter forskriftens § 6-7, hva som menes med bakgrunnssjekk, egnethetsvurdering og kredittsjekk, og hvordan kravene til personkontrollen kan oppfylles.

Dette er krav som også universiteter og høgskoler må imøtekomme dersom deres personell skal inngå i vitenskapelig forskningssamarbeid innenfor samfunnsviktige tjenester som omfattes av slike regelverk. Gjennom forskningssamarbeid kan personellet få tilgang eller adgang til, og dyp innsikt i, nettverks- og informasjonssystemer, eller klassifiserte anlegg og systemer. Det vil være nødvendig med gode avklaringer med samarbeidende virksomhet, slik at eventuelle krav til sikkerhetsmessig egnethet er proporsjonale og hensiktsmessige, og at ansvar for sikkerhetsopplæring og kompetanse, og for sikkerhetsmessig oppfølging i arbeidsforholdet er tydelig fordelt.

[64] Veileder fra NSM i digitalsikkerhetsloven og -forskriften.pdf
[65] https://veiledere.nve.no/kraftberedskapsforskriften/kapittel-6-informasjonssikkerhet/6-7-personkontroll/

Digitalsikkerhetsloven med forskrift, stiller krav til at personell som skal ha adgang eller tilgang til nettverk og informasjonssystemer til tjenester som loven omfatter, skal være pålitelige og ha tilstrekkelig kompetanse.

Kraftberedskapsforskriften stiller krav til KBO-enheter om å gjennomføre bakgrunnssjekk før ansettelse.

Personlig sikkerhetsmessig egnethet vil være nødvendig å vurdere, og må knyttes til forhold som arbeidsgiver kan undersøke.

Universiteter og høgskoler bør kjenne til hvordan disse bestemmelsene kan bli aktuelle ved samarbeid med virksomheter som per i dag er underlagt dette regelverket, og kan måtte imøtekomme slike personellmessige sikkerhetskrav for sine ansatte.

4.9 Andre tungtveiende sikkerhetshensyn

Tungtveiende sikkerhetshensyn er et uttrykk hentet fra saker behandlet av Diskrimineringsnemda. Denne veilederen velger å bruke *Andre tungtveiende sikkerhetshensyn* som kategori-benevnelse på fagområder med verdier som ikke er (direkte) beskyttet gjennom lover og forskrifter, men hvor personellmessige sikkerhetstiltak likevel kan være nødvendige.

I *Sikkerhetsfaglig råd* sier NSM at enkelte verdier kan være *særskilt utsatt for sikkerhetstruende virksomhet*[66], at slik virksomhet gjerne skjer fordekt og at det kan være vanskelig å avdekke hvem som står bak. For UH-virksomheter kan dette handle om fag- og teknologiområder som er særlig viktige for norske interesser, sikkerhetsinteresser og utviklingsevne, og om tilganger til databaser, registre, informasjon og administratorrettigheter. Verdier i UH-sektoren som er *særskilt utsatt for sikkerhetstruende virksomhet* kan trues av fremmed etterretning og andre aktørers aktivitet enten direkte, eller indirekte gjennom flere ledd, og av ulike former for påvirkning og innblanding som forskere kan utsettes for innenfor enkelte fagområder.

[66] Sikkerhetsfaglig råd - Et motstandsdyktig Norge.pdf

Forskningssikkerhet[67] legger vekt på identifiseringen og håndteringen av risiko knyttet til uønsket kunnskaps- og teknologioverføring, uønsket påvirkning og innblanding, samt brudd på forskningsetikk og faglig integritet gjennom bruk av kunnskap og teknologi til å underminere sentrale samfunnsverdier

Disse risiko-områdene er særlig viktige å vurdere i internasjonalt samarbeid, og utdypes nærmere i Meld. St. 14 (2024-2025):

Risiko for uønsket kunnskapsoverføring er nært knyttet til nasjonal sikkerhet ved at kunnskap om flerbruksvarer og teknologi som kan være eksportkontrollregulert, eller andre strategiske, kritiske eller sensitive teknologier kan havne i stater som i et verstefallsscenario benytter slik teknologi imot oss eller våre nærstående land.

Risiko for påvirkning og innblanding er mer knyttet til humaniora og samfunnsfag, og til utfordringer som angår akademisk frihet, som at forskere tilpasser forskningen på grunn av politiske restriksjoner i samarbeidsland, eller at statlige aktører påvirker forskning for å fremme egne interesser. Konsekvenser kan være innskrenket akademisk frihet, berørte forskeres liv og helse, og påvirkning eller forstyrrelse av pågående demokratiske prosesser.

Risiko for brudd på forskningsetikk knyttes særlig til at ulike land forstår og følger opp forskningsetiske prinsipper på ulike måter. Faglig integritet kan komme under press gjennom selvsensur, og forskere kan oppleve etiske dilemmaer i samarbeid med land i konflikt og/eller med andre politiske styresett. Dette kan føre til brudd på forskningsetikken og få konsekvenser for berørte forskeres liv og helse.

Forskning kan påvirkes eller utsettes for sikkerhetstruende virksomhet i en slik grad at det får konsekvenser for våre grunnleggende samfunnsverdier, som forskningsetikk, akademisk frihet og ytringsfrihet, så vel som for nasjonale interesser innen økonomi og sikkerhet. Sikkerhetstruende virksomhet kan også ha konsekvenser for enkelte ansattes arbeidsforhold og helse, og for berørte arbeidsmiljø.

[67] Meld. St. 14 (2024–2025) - regjeringen.no

4.9.1 Særlig om sensitive teknologier og flerbruksteknologi

Gjennom *Kunnskapsgrunnlag for vurdering av sensitive teknologier* (KVAST)[68] er det etablert et mer helhetlig kunnskapsgrunnlag om hvilke teknologiområder og hvilke konkrete teknologier som er såkalt særlig *sensitive*. Vurderingene er gjort opp mot nasjonal sikkerhet for å sikre:

- Fortsatt åpenhet på områder hvor faglig samarbeid er ønskelig og viktig i lys av kunnskapspolitiske mål – inkludert Norges langsiktige kunnskaps- og kompetansebehov – og hvor eventuell risiko vurderes som håndterbar og dermed akseptabel.
- Å redusere risiko til et akseptabelt nivå på områder som er i gråsonen.
- Å unngå samarbeid på områder hvor risikoen vurderes som ikke-akseptabel.

KVAST sin delleveranse 2[69] (s. 7) beskriver sensitive teknologier som teknologier som ved tilegnelse fra uønskede aktører, vil kunne påvirke norske sikkerhetsinteresser og teknologisk konkurranseevne negativt.

Sensitive teknologier bør derfor beskyttes av personellmessige sikkerhetstiltak, så vel som fysiske og tekniske.

KVAST sin del-leveranse 4[70] sier at kunnskapsgrunnlaget som etableres skal bidra til å

- Redusere risiko forbundet med sensitive teknologier (beskytte);
- Sikre tilstrekkelig norsk kunnskap og kompetanse på teknologiområder av betydning for nasjonal sikkerhet (fremme);
- Tilrettelegge for ansvarlig internasjonalt samarbeid, som sikrer trygge rammer for samarbeid, også med land vi ikke har et sikkerhetspolitisk samarbeid med (samarbeide).

[68] https://www.forskningsradet.no/forskningspolitikk-strategi/forskningssikkerhet/kvast/
[69] https://www.forskningsradet.no/contentassets/7bd23b01e42146acbb23d256113a2246/kvast-delleveranse-2.pdf
[70] https://www.forskningsradet.no/contentassets/7bd23b01e42146acbb23d256113a2246/kvast-delleveranse-4.pdf

KVAST har etablert en metodikk for å vurdere risiko knyttet til de sensitive teknologiene som benytter følgende kriterier:

- Eksponering for utenlandske aktører
- Regulatorisk kontroll og etterlevelse
- Potensiell militær eller strategisk utnyttelse
- Konsekvenser for kritisk infrastruktur
- Økonomisk sikkerhet
- Respekt for menneskeverd

Hver av disse seks kriteriene er i delleveranse 4 utredet for enkelte av de utpekte sensitive teknologiområder, og gitt et nivå fra 1-4.

Denne veilederen anbefaler å se til denne metodiske tilnærmingen for å løpende vurdere egne teknologier sin «sensitivitetsgrad». Som KVAST-leveransene viser, vil sensitive teknologier kunne *ha eller få* betydning for nasjonale sikkerhetsinteresser, de *kan være eller trolig bli* regulert av eksportkontrollen og sanksjoner, og de vil kunne *ha eller få* betydning for samfunnsviktige tjenester og samfunnskritiske funksjoner som eksempelvis kraftsektoren.

Denne veilederen viser også til virksomhetenes nivåer for klassifisering av informasjon. *Konfidensialitetsklassifisering*[71] av informasjon som ikke er sikkerhetsgradert etter sikkerhetsloven, klassifiseres gjerne som såkalt «røde» eller «sorte data». Røde og sorte data medfører streng tilgangs- og adgangskontroll, og må også medfører både digitale, fysiske og personellmessige sikkerhetstiltak for å redusere risiko helhetlig (jfr. Beskyttelsesinstruksen § 12)[72].

Dersom *sikkerhetsgradering* er aktuelt, må KD orienteres og NSM kontaktes for videre oppfølging.

[71] Se til Sikt sin veiledning og sektorstandard for klassifisering av informasjon
[72] https://lovdata.no/forskrift/1972-03-17-3352/§4 https://lovdata.no/forskrift/1972-03-17-3352/§12

4.9.2 Andre tungtveiende sikkerhetshensyn og personellsikkerhet

Felles for alle som jobber med sikkerhetsgradert informasjon, eksportkontrollregulert teknologi, eller med verdier som medfører andre tungtveiende sikkerhetshensyn, er at de ansatte selv er et mulige mål for etterretningsaktører eller andre som ønsker å utnytte deres tilganger til disse verdiene.

Arbeidsgiver må ha gode systemer for opplæring og oppfølging av ansatte og tilknyttede gjennom hele ansettelsesforholdet, slik at de forstår at de må bidra til god sikkerhet. Nærmeste leder bør kjenne til eventuelle sårbarheter ved sine ansatte, som med en viss sannsynlighet vil kunne bli forsøkt utnyttet av aktører som ønsker tilgang til verdiene de behandler, og følge opp på en god måte som ivaretar den ansatte og beskytter verdiene.

Det er derfor nødvendig risikohåndtering å vurdere og følge opp om *personlig sikkerhetsmessig egnethet* ved rekruttering og videre oppfølging, selv når det ikke kommer direkte av lovbestemmelser.

Andre tungtveiende sikkerhetshensyn kan medføre behov for å vurdere personlig sikkerhetsmessig egnethet ved rekruttering og oppfølging. Personlig sikkerhetsmessig egnethet vil være nødvendig å vurdere, og må knyttes til forhold som arbeidsgiver kan undersøke.

Universiteter og høgskoler bør gjøre grundige og konkrete vurdering av hvilke verdier de har som kan være utsatt for sikkerhetstruende virksomhet i en slik grad at personellmessige sikkerhetstiltak vil være nødvendig.

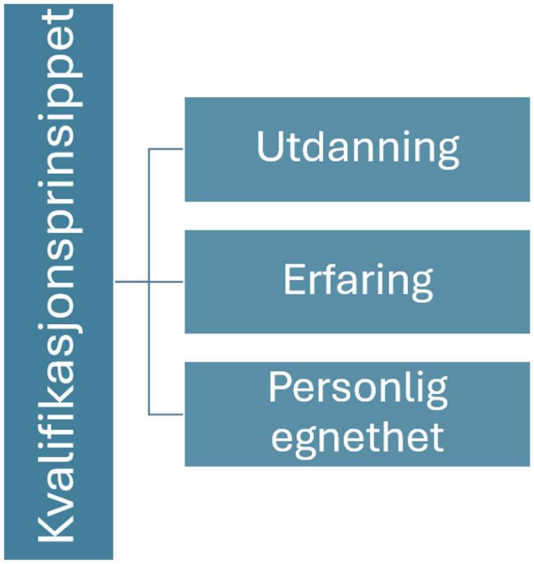
4.10 Personlig sikkerhetsmessig egnethet som kvalifikasjonskrav

I den statlige arbeidsgiverpolitikken er Statens personalhåndbok[73] (SPH) et oppslagsverk over de sentrale bestemmelsene, og brukes som et verktøy for å forstå og praktisere disse. Blant annet redegjøres det i SPH for *kvalifikasjonsprinsippet*, som bygger på grunnleggende prinsipper om likebehandling, rettferdighet og saklighet.

[73] Statens personalhåndbok - regjeringen.no

4.10.1 Kvalifikasjonsprinsippet

Ansettelser i staten skal følge forvaltningslovens saksbehandlingsregler og de alminnelige kravene til forsvarlig saksbehandling etter ulovfestede forvaltningsrettslige prinsipper.



Kvalifikasjonsprinsippet sier at søkeren som er best kvalifisert for en stilling skal ansettes gjennom vurdering basert på *utdanning*, *erfaring* og *personlig egnethet*.

Denne vurderingen må være sammenholdt med kvalifikasjonskravene som er fastsatt i den konkrete utlysningsteksten.
Basert på sikkerhetskrav knyttet til arbeidets innhold, vil det i enkelte tilsettingssaker være nødvendig å med krav knyttet til *kandidatens sikkerhetsmessige egnethet*.

Vurdering av sikkerhetsmessig egnethet vil da inngå som en del av vurderingen av *personlig egnethet*.

Slike vurderinger må være knyttet til stillingens innhold og eventuelle tjenstlige behov, og må dokumenteres skriftlig med hensyn til relevant lovverk eller andre sikkerhetsmessige vurderinger av betydning. For å ivareta hensynet til etterprøvbarhet skal det fremgå av dokumentene som danner grunnlaget for innstillingen at det er gjort en individuell og helhetlig vurdering av aktuelle søkere.

Som gjennomgangen av regelverkene viser, så er det ulikt hvilke nivåkrav til sikkerhetsmessig egnethet som stilles direkte fra lov og forskrift, hvem som gjennomfører undersøkelsene og vurderingene, hvor omfattende slike undersøkelser skal være, og hvilket samtykke som kreves.

Kategori 1: Sikkerhetsklarering og autorisasjon (etter sikkerhetsloven)
For såkalt personkontroll knyttet til vurdering av *sikkerhetsmessig skikkethet* og klareringer regulert av lov og forskrifter for nasjonal sikkerhet, er kravene definerte og gjennomføres av Sivil klareringsmyndighet, den autorisasjonsansvarlige i virksomheter, og i enkelte tilfeller med involvering av Nasjonal sikkerhetsmyndighet.

Kategori 2: Lisens og tillatelser (etter eksportkontroll- og sanksjonsregelverket)
For behandling av *søknad om lisens og tillatelser* iht eksportkontrollregelverket og sanksjonsforskriftene, er det DEKSA som vurderer og behandler hver søknad individuelt.

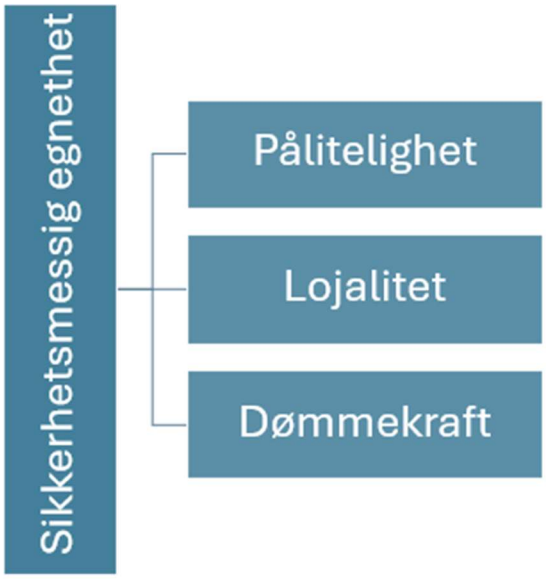
Kategori 3: Sikkerhetsmessig egnethet (av andre tungtveiende sikkerhetshensyn)
For personellmessige sikkerhetstiltak omfattet av Digitalsikkerhetslov med forskrift, eller for personkontroll omfattet av kraftberedskapsforskriften, eller for personellmessige vurderinger knyttet til andre tungtveiende sikkerhetshensyn, vil det være arbeidsgiver selv som i stor grad må definere slike tiltak.

4.11 Pålitelighet, lojalitet og dømmekraft

Hvilke vurderinger av hvilke forhold som er av betydning for en person sin sikkerhetsmessige egnethet i den enkelte rekrutteringssak, bør følge konsekvente og lovlige kriterier og metoder for undersøkelse og vurdering. Dette er viktig både for å opprettholde et saklighetsnivå, og en lik behandling av søkerne.

Gjennomgangen av regelverkene har synliggjort at det ikke fremmes krav til, eller kriterier for sikkerhetsmessige vurderinger i universitets- og høgskoleloven eller i statsansatteloven, som kan komme til anvendelse for UH-virksomhetene.

Denne veilederen tilstreber å komme frem til en viss standardisering av vurdering av sikkerhetsmessig egnethet av personell for UH-virksomhetene utenfor sikkerhetsloven, ved å overføre kriterier og metoder for undersøkelser og vurderinger fra de aktuelle regelverk som er gjennomgått.



Personlig sikkerhetsmessig egnethet handler i bunn og grunn om en person sin *lojalitet, pålitelighet og dømmekraft* knyttet til forhold av mulig betydning for sikkerheten. Graden av krav til slike egenskaper vil klart henge sammen med beskyttelsesbehovet til verdiene som arbeidets innhold vil gi.

I lys av sikkerhetsmessig egnethet forstås slike egenskaper som viktige for å kunne ivareta sikkerheten til de verdier som arbeidets innhold medfører, og for å redusere sannsynlighet for såkalt *innsiderisiko*. Dette vil være viktig både i forbindelse med rekruttering av nye ansatte, og i oppfølging av det personellet som allerede er i virksomheten.

For å vurdere sikkerhetsmessig egnethet ut fra disse egenskapene, vil det være nødvendig å ha informasjon om forhold som er av en slik betydning at de kan påvirke personens pålitelighet, lojalitet og dømmekraft knyttet til sikkerheten.

Dette møter raskt åpenbart komplekse og sammensatte forhold som vil kunne være i endring og i faser, og hvor det vanskelig lar seg gjøre å trekke tydelige sammenhenger. Slike forhold kan handle både om den enkelte sin personlighet, private og profesjonelle bakgrunn og tilknytninger, helse og økonomi, og sosiokultur og etnisitet. Det handler også om personens forhold til rutiner for sikkerhet som tilgangsstyring, adgangskontroll, sikkerhetsmessige ledelse, arbeidsmiljø og ledertetthet. Det vil ofte være vanskelig å skille mellom hvilke forhold som vil kunne påvirke hvilken egenskap hos den enkelte person.

I FFI-rapporten *Hva vet vi om innsiderisiko*[74] (s. 24) står det at «for å være i stand til å stole på en person eller en organisasjon må en ha grunnlag for å tro på at de har velmenende og

[74] Hva vet vi om innsiderisiko?

vennlige holdninger, er i stand til å gjøre det en forventer av dem, opptrer ærlig og rettferdig i møte med andre, og er konsekvente i sine handlinger i form at de gjør det de sier at de skal gjøre.»

SINTEF-rapporten *En metastudie om innsidetrusselen*[75] (s. 24) sier at psykologisk profilering av mulige innsidere er etterspurt og i utgangspunktet en appellerende idé, men i realiteten vanskelig å få til. Rapporten peker på atferdspsykologien som vektlegger at det vil være mer produktivt å trekke på psykologiske verktøy som oppfordrer til ønsket atferd blant ansatte, enn å lete etter personlighetstrekk som narsissisme, machiavellisme og psykopati, og avvikende og antisosial atferd.

Med dette som bakteppe tar veilederen utgangspunkt i hva som per i dag er vanlig praksis i norsk arbeidsliv å undersøke, og forslår hvordan UH-virksomhetene kan undersøke forhold av betydning for sikkerhetsmessig egnethet knyttet til UH-virksomheters aktivitet.

4.12 Forhold av betydning for sikkerhetsmessig egnethet

4.12.1 Sikkerhetsbevissthet og risikoerkjennelse

Til alle stillinger med krav til personlig sikkerhetsmessig egnethet vil det være nødvendig å vurdere kandidatens sikkerhetsbevissthet og risikoerkjennelse. Dette handler blant annet om holdning og forståelse til risiko og sikkerhetstiltak, og kan vurderes i rekrutteringssammenheng gjennom å stille spørsmål for refleksjon over relevante temaer.

Slike forhold kan ha mulig betydning for personens *dømmekraft og pålitelighet* knyttet til ivaretakelse av verdiene.

4.12.2 Landtilknytning

Til alle stillinger med krav til personlig sikkerhetsmessig egnethet vil det være hensiktsmessig å vurdere kandidaten sine landtilknytninger. Dette handler om å kunne håndtere risiko for blant annet kunnskapsspionasje, ved at en ansatt kan bli utsatt for press eller andre former for tilnærminger fra fremmed etterretning. Det handler også om å kunne ivareta den ansatte.

Landtilknytning kan ha mulig betydning for personens *lojalitet* knyttet til ivaretakelse av verdiene.

[75] En metastudie om innsidetrusselen - SINTEF

4.12.3 Andre tilknytninger

Til alle stillinger med krav til personlig sikkerhetsmessig egnethet vil det være nyttig å undersøke personens sampubliseringer og annet vitenskapelig samarbeid, eventuelle næringsinteresser, finansieringsforbindelser, eller andre tilknytninger eller forbindelser som kan ha en betydning.

Slike forhold kan ha mulig betydning for personens *pålitelighet og lojalitet* knyttet til ivaretakelse av verdiene.

4.12.4 Kredittsjekk

Til enkelte stillinger med krav til personlig sikkerhetsmessig egnethet vil det være hensiktsmessig å gjennomføre kredittsjekk. Det gjelder spesielt for stillinger med administratorrettigheter i store systemer, budsjettmyndighet, eller andre roller som innebærer store systemtilganger og ansvar.

Negative skårer i en kredittsjekk kan ha mulig betydning for personens *pålitelighet og lojalitet* knyttet til ivaretakelse av verdiene.

4.12.5 Andre grunnleggende sikkerhetstiltak

For alle stillinger, og spesielt for alle stillinger med krav til personlig sikkerhetsmessig egnethet, bør det gjennomføres identitetskontroll og verifikasjon av dokumentasjon og bakgrunn.

Hvordan slike undersøkelser av sikkerhetsmessig egnethet, ID-kontroll, og verifikasjon av dokumentasjon og bakgrunn i praksis kan gjennomføres og vurderes, foreslås i Del 2 i veilederen.

4.13 Behandlingsgrunnlag for gjennomføring av bakgrunnssjekk

Det er begrenset med (norske) autoritative rettskilder som handler om bruken av ulike behandlingsgrunnlag til å gjennomføre bakgrunnssjekk av kandidater før ansettelse. Det finnes likevel noe juridisk teori nasjonalt og innen EU om temaet.

Et eksempel fra tysk rett[76]

"The LAG Düsseldorf held that searching for the applicant's name on a well-known online search engine was permitted under Article 6(1)(b) GDPR (performance or initiation of a contract, here the potential employment relationship). The court argued that if the pre-contractual measure — like in this case — can be traced back to the initiative and intention of the data subject, Article 6(1)(b) GDPR permits the collection and processing of data to the extent necessary for the specific selection process. According to the LAG Düsseldorf, it was necessary for the specific selection process because it is the duty of a public employer to determine and verify the suitability of applicants."

https://www.orrick.com/en/insights/2025/10/navigating-employee-privacy-key-takeaways-from-recent-damages-claim-under-the-gdpr

Å innhente personopplysninger i forbindelse med en bakgrunnssjekk må være nødvendig for å ivareta arbeidsgiverens legitime interesser. Opplysningene skal være relevante for å vurdere hvilken risiko personen kan utgjøre, knyttet til arbeidets innhold. Adgangen til å innhente politiattest er lovregulert med særlige vilkår i politiregisterloven.

Behandlingsgrunnlagene som listes opp under er hentet fra juridisk utredning fra KS[77] og artikkel fra Lov & Data[78]:

GDPR artikkel 6 nr. 1, bokstav f. om berettiget interesse

- Denne er mye brukt som behandlingsgrunnlag for å gjennomføre bakgrunnssjekk ved rekruttering, og er lovlig dersom arbeidsgiver kan dokumentere at behovet for å gjennomføre en slik undersøkelse veier tyngre enn kandidatens vern av personopplysninger.
- Vurderingen av behovet for en bakgrunnssjekk må gjøres på forhånd for den enkelte stillingen som skal besettes.

[76] https://www.orrick.com/en/insights/2025/10/navigating-employee-privacy-key-takeaways-from-recent-damages-claim-under-the-gdpr
[77] https://www.ks.no/ks-advokatene/nyheter/behandlingsgrunnlag-for-bakgrunnssjekk-ved-ansettelser/
[78] https://lod.lovdata.no/article/2025/03/Behandlingsgrunnlag%20for%20bakgrunnssjekk%20ved%20ansettelser

- Ved rekrutteringen er det normalt kun lovlig å gjennomføre en bakgrunnssjekk av kandidatene som det er aktuelt å gi tilbud om ansettelse, og ikke av alle søkerne.
- Dette behandlingsgrunnlaget dekker ordinære personopplysninger, og ikke opplysninger i særlige kategorier etter GDPR artikkel 9.

GDPR artikkel 6 nr. 1, okstav b. om avtaleinngåelse eller avtaleoppfyllelse

- Denne kan benyttes som behandlingsgrunnlag for å gjennomføre bakgrunnssjekk ved rekruttering ved å vise til at formålet er å inngå en arbeidsavtale, og arbeidsgiver har vurdert det som nødvendig å gjennomføre en bakgrunnssjekk av aktuelle kandidater før avtaleinngåelsen.
- Dette grunnlaget dekker også særlige kategorier av personopplysninger, jf. personopplysningsloven § 6 og GDPR art. 9 nr. 2 bokstav b. Forutsetningen er at arbeidsgiver vurderer bakgrunnssjekken som en del av sine forpliktelser knyttet til å ansette den beste kandidaten til stillingen.
- Åpenhet om kravene i utlysningsteksten fungerer som forventningsavklaring til kandidatene om hvor grundige bakgrunnsundersøkelser som vil bli foretatt i rekrutteringsprosessen.

4.14 Sikkerhetsvurderinger og diskrimineringsvernet

Spørsmål knyttet til statsborgerskap, landtilknytning og etnisitet har blitt mer aktuelt i norsk arbeidsliv, særlig som følge av krigen i Ukraina og trusselbildet for øvrig. Dette gjelder også for universiteter og høgskoler.

I rapport fra Likestillings- og diskrimineringsombudet (LDO) *Diskrimineringsretten 2023*[79], kapittel 2.6 om *Sikkerhetsvurderinger i arbeidsforhold og forholdet til diskrimineringsvernet*, gis en gjennomgang av hvilke type henvendelser fra enkeltpersoner og virksomheter som LDO får knyttet til sikkerhetsvurderinger av arbeidssøkere og ansatte. Det anbefales å lese LDOs rapport, og særlig nevnte kapittel fra s. 36-41.

[79] https://ldo.no/content/uploads/2024/06/Diskrimineringsretten-2023.pdf

Et rettsområde i bevegelse

Dette er et rettsområde i bevegelse, og det er nødvendig at virksomhetene holder seg oppdaterte på hvordan Diskrimineringsnemda[80] behandler saker som de får inn, i tillegg til hvilke nye vurderinger og tolkninger som kommer fra LDO.

Bistand fra (eksterne) advokater kan gi råd og vurderinger som gir litt ulike retninger.

Veilederen tar ikke stilling til ulike retninger, men har til hensikt å vise hvilke vurderinger som må gjøres, og hvilke momenter som må inngå i vurderingene.

Under gjengis deler av Likestillings- og diskrimineringsombudet (LDO) veiledning om sikkerhetsvurderinger i arbeidsforhold[81]:

Vår veiledning

Det å vektlegge en arbeidssøkers etnisitet i en ansettelsesprosess, reiser spørsmål om diskriminering etter likestillings- og diskrimineringsloven. Statsborgerskap er ikke i seg selv et vernet diskrimineringsgrunnlag etter likestillings- og diskrimineringsloven, men i arbeidslivet vil vektlegging av statsborgerskap regnes som indirekte forskjellsbehandling på grunn av etnisitet, se for eksempel Diskrimineringsnemndas sak 2022/782[82].

Som redegjort for over, er både eksisterende, tidligere og antakelser om etnisitet/statsborgerskap omfattet av diskrimineringsforbudet. Også avledet etnisitet, altså vektlegging av tilknytning til en person med en viss etnisk bakgrunn, er omfattet av diskrimineringsforbudet, jf. ldl. § 6 tredje ledd.

For selve vurderingen av diskriminering må vi skille mellom stillinger der det er krav om sikkerhetsklarering i lov (som sikkerhetsloven) og stillinger der det ikke er et krav om sikkerhetsklarering.

Krav om sikkerhetsklarering i lov

Der krav om statsborgerskap, landbakgrunn e.l. følger av lov (for eksempel sikkerhetsloven § 8-4 fjerde ledd), blir det som hovedregel ikke et spørsmål om

[80] Søk i klagesaker | Diskrimineringsnemnda.no
[81] Se Vedlegg x hele brevet
[82] 21-771-offentlig-versjon-av-vedtak.pdf

diskriminering. Det kan da være lovlig for klareringsmyndigheten å vektlegge statsborgerskap/landbakgrunn e.l. i henhold til sikkerhetslovens bestemmelser om dette.

Hvis det er krav om sikkerhetsklarering for å få en stilling, kan en arbeidsgiver bruke manglende sikkerhetsklarering som grunnlag for å avslå en jobbsøknad eller oppsigelse av en ansatt, selv om etnisitet/nasjonal opprinnelse har hatt betydning for klareringsmyndighetens vurdering. Sikkerhetsklarering blir i slike tilfeller å anse som et kvalifikasjonskrav for å få stillingen.

Når det gjelder arbeidsgivers anledning til å vektlegge antakelser om hvorvidt en arbeidssøker vil få klarering eller ikke, mener ombudet at det følger av diskrimineringsvernet at arbeidsgivere bør være forsiktige med å basere seg på slike antakelser før sikkerhetsmyndighetene har foretatt sin vurdering. I nemndspraksis har det avgjørende i slike tilfeller vært om arbeidsgiver kan sannsynliggjøre at søkeren ikke vil få den sikkerhetsklareringen som kreves.

Her finnes det relevant praksis fra Diskrimineringsnemnda:

Sak 2022/782[83]

Saken gjaldt en polsk statsborger som søkte på en stilling der det var krav om sikkerhetsklarering. Arbeidsgiveren mente at søkeren ikke ville få sikkerhetsklarering tidsnok til å kunne ansettes. Nemnda kom til at arbeidsgiveren ikke hadde sannsynliggjort at søkeren ikke ville få klarering, og at arbeidssøkeren var diskriminert. Her hadde arbeidsgiveren for øvrig også oppstilt et krav om norsk statsborgerskap for å få stillingen. Til dette sier nemnda at et slikt kategorisk krav ikke er forholdsmessig fordi Sivil klareringsmyndighet foretar en konkret vurdering i hver enkelt sak.

Sak 2022/1093[84]

Denne saken gjaldt spørsmål om en arbeidsgiver hadde lovlig adgang til å innhente og vektlegge opplysninger om en arbeidssøkers ektefelle sin nasjonalitet, før den formelle klareringsprosessen ved Sivil klareringsmyndighet var gjennomført.

Etter en konkret vurdering konkluderte nemnda med at arbeidssøkeren ikke var diskriminert og at arbeidsgiveren hadde adgang til å innhente og vektlegge opplysningene om arbeidssøkerens ektefelle. I vurderingen la nemnda blant annet vekt på at

[83] 21-771-offentlig-versjon-av-vedtak.pdf
[84] 22-1093-offentlig-versjon-av-uttalelse.pdf

sikkerhetsklarering var en forutsetning for å kunne tiltre stillingen og at den aktuelle opplysningen gjaldt forhold som med svært stor sannsynlighet ville kunne forutsi utfallet av klareringssøknaden.

Nemnda la vekt på at «både arbeidstaker og arbeidsgiver vil bli satt i en uforholdsmessig usikker situasjon dersom et arbeidsforhold må startes selv om vedkommende med stor sannsynlighet ikke kan tiltre stillingen grunnet manglende sikkerhetsklarering.» Nemnda mente at det var mindre inngripende for arbeidstaker at arbeidsavtalen ble hevet før tiltredelse enn etter arbeidsforholdet hadde startet.

Stillinger uten formelle krav om sikkerhetsklarering

Når det ikke er lovhjemlet krav om sikkerhetsklarering, må arbeidsgivere kunne vise til at de har foretatt en konkret vurdering av den spesifikke sikkerhetsrisikoen knyttet til personens landbakgrunn, og denne må ha avgjørende betydning for utøvelsen av arbeidet eller yrket, jf. ldl. § 9.

Generelt skal det mye til for at vilkåret «avgjørende betydning» er oppfylt. I tillegg må forskjellsbehandlingen være nødvendig for å oppnå et saklig formål og forholdsmessig overfor den som forskjellsbehandles.

Sikkerhetshensyn er som regel saklige formål etter likestillings- og diskrimineringsloven.

Når det gjelder kravet om nødvendighet, blir spørsmålet om sikkerhetshensynene kan ivaretas på annen, mindre inngripende måte enn ved å forskjellsbehandle arbeidssøkeren eller den ansatte. Dette kan stille krav om at arbeidsgiveren vurderer muligheten for å tilpasse arbeidsoppgaver eller begrense tilganger til systemer/objekter.

Se for eksempel Diskrimineringsnemndas sak DIN-23-552, som illustrerer hvilke vurderinger som gjøres i slike saker. I denne saken uttalte nemnda at de konkrete sikkerhetsinteressene som arbeidsgiver oppgir må være «relevante i den foreliggende saken og bygge på riktig faktisk grunnlag.

Når det gjelder personer som allerede er ansatt, vil kravet om forholdsmessighet kunne skjerpe kravet til at arbeidsgiver må forsøke å finne løsninger som innebærer minst mulig inngrep overfor den ansatte, som at arbeidsgiver må vurdere å iverksette tiltak for å redusere sårbarheten knyttet til konkrete personer.

Se for eksempel DIN-23-68, der nemnda sier seg enig med arbeidsgiveren i at forholdsmessighetsvurderingen av personer som allerede er ansatt, er en annen enn vurderingen av arbeidssøkere til en stilling. I den saken hadde arbeidsgiveren «iverksatt

en rekke til dels ressurskrevende tiltak for å redusere sårbarhet knyttet til ansatte som kan være attraktive etterretningsmål for utenlandske etterretningstjenester.

Ombudets råd til arbeidsgivere

Det er flere faktorer enn landbakgrunn som kan utgjøre en sikkerhetsrisiko. For å unngå et ensidig fokus på statsborgerskap og landbakgrunn, mener ombudet at arbeidsgivere ikke kun bør vurdere sikkerhetsrisiko/sårbarheter i form av tilknytning til visse land, men at det vil være klokt av arbeidsgivere å tenke helhetlig på hva som kan utgjøre sikkerhetsrisikoer.

4.14.1 Om statsborgerskap og etnisitet

Etnisitet og nasjonal opprinnelse er ikke ensbetydende med statsborgerskap. Dette er slått fast i forarbeidene til sikkerhetsloven, Prop. 81 L (2016-2017) punkt 11.2.3.3. Det følger videre av forarbeidene på samme sted at forskjellsbehandling på grunn av statsborgerskap vil kunne rammes av forbudet mot indirekte diskriminering på grunn av etnisitet.

Sivil klareringsmyndighet påpeker at et *statsborgerskap* fra visse stater *alene* ikke vil være grunn nok til å utelukke en søker fra en videre rekrutteringsprosess. Dette bør derfor anses som hovedregel hvor personlig sikkerhetsmessig egnethet skal vurderes. Det skal alltid gjøres en konkret og individuell vurdering av stillingssøkeren som person.

I helhetsvurderingen av om personen er sikkerhetsmessig skikket, er ingen opplysninger eller forhold automatisk ekskluderende. En person kan være utvandret fra en stat som lite barn og formelt fortsatt være statsborger av staten, fordi man etter statens lovgivning bare kan løses fra statsborgerskapet etter vedtak fra myndigheten i staten. Flere slike personer har blitt sikkerhetsklarert i Norge, etter en konkret og individuell helhetsvurdering av personens sikkerhetsmessige skikkethet.

For ytterligere informasjon om dette temaet, se sikkerhetsloven § 8-4 fjerde ledd om tilknytning til andre stater og NSMs veileder i personellsikkerhet kap. 2.4, samt loven § 8-7 om klarering av personer med utenlandsk statsborgerskap og NSMs veileder i personellsikkerhet kap. 2.7.

4.14.2 Eksempler på saker fra Diskrimineringsnemda

I vedtak fra sakene 22/1093[85] og 2023/552[86] kommer det frem hvordan Diskrimineringsnemda har vurdert *tungtveiende sikkerhetshensyn* som grunnlag for forskjellsbehandling, og hvordan samtlige fire vilkår i § 9 om lovlig forskjellsbehandling er oppfylt.

I vedtak fra sak 2023/535[87] kommer det frem hvordan Diskrimineringsnemda har vurdert at en forskjellsbehandling med bakgrunn i *etnisitet* var ulovlig, ved at vilkårene i § 9 ikke er oppfylt.

I vedtak fra sak 2024/223[88] kommer det frem hvordan Diskrimineringsnemda har vurdert at klager var utsatt for direkte forskjellsbehandling på grunn av etnisitet, fordi det ikke var gjort en konkret og individuell vurdering av klager. I denne saken forelå det et saklig hensyn for å stille krav til autorisasjonsprosess, men det var ikke saklig, nødvendig og forholdsmessig å la være å gå videre med klager fordi en autorisasjonsprosess ville være tidkrevende. Et viktig moment i denne saken, er at nemnda understrekte i avgjørelsen at den ikke har tatt, eller skal ta, stilling til hva et eventuelt resultat fra en autorisasjonsvurdering ville blitt.

4.14.3 Eksempler på saker om sikkerhetsklarering behandlet av domstolene

Hvis en person som har fått stilling med krav om sikkerhetsklarering, ikke får sikkerhetsklarering, kan arbeidsavtalen sies opp om ikke andre alternative oppgaver kan erstatte det planlagte arbeidsinnholdet.

Det vil også være et saklig grunnlag for å si opp en statsansatt dersom stillingen krever sikkerhetsklarering og den ansatte mister klareringen. I så fall vil ikke den ansatte lenger ha *«de kvalifikasjoner som er nødvendig eller foreskrevet for stillingen»,* jf. statsansatteloven § 20 første ledd bokstav b.

Dette er også slått fast av Borgarting lagmannsrett i saken med referanse LB-2018-186121[89]. Saken gjaldt en ansatt i Forsvaret som mistet sikkerhetsklareringen, hvor

[85] https://www.diskrimineringsnemnda.no/media/9019/22-1093-offentlig-versjon-av-uttalelse.pdf
[86] https://www.diskrimineringsnemnda.no/media/yexar0vr/23-552-ytterligere-anonymisert-offentlig-versjon-av-uttalelse.pdf
[87] https://www.diskrimineringsnemnda.no/media/ixpnelzr/offentlig-versjon-av-vedtak.pdf
[88] Sak #24/223 | Diskrimineringsnemnda.no
[89] Borgarting lagmannsrett - Dom og kjennelse: LB-2018-186121 - Lovdata

domstolen slo fast at *«Det er ubestridt at sikkerhetsklarering er en nødvendig kvalifikasjon for As stilling. Tap av sikkerhetsklarering medfører dermed at lovens vilkår om at arbeidstager ikke lenger har de nødvendige kvalifikasjoner for stillingen i utgangspunktet er oppfylt»*. Saken ble nektet fremmet til Høyesterett.

Videre kan både tilknytning til andre stater og den geopolitiske situasjonen vektlegges i forbindelse med vurderingen av om en person kan få sikkerhetsklarering. Det første følger direkte av sikkerhetsloven § 8-4 fjerde ledd bokstav n, som sier at en persons tilknytning til andre stater kan tillegges vekt.

Spørsmålet om betydningen av den geopolitiske situasjonen er behandlet av Borgarting lagmannsrett i saken med referanse LB-2023-119522[90]. Saken gjaldt gyldigheten av et avslag på sikkerhetsklarering som følge av at saksøkeren hadde russisk ektefelle. Saksøkeren hadde tidligere vært sikkerhetsklarert, men SKM la vekt på hvordan den geopolitiske situasjonen har endret seg, og hvilken sikkerhetsmessig bevissthet vedkommende hadde utvist. Lagmannsretten opprettholdt avslaget.

[90] Borgarting lagmannsrett - Dom: LB-2023-119522 - Lovdata

Referanser og kilder

(ikke fullstendig ved høring)

https://www.regjeringen.no/no/dokumenter/styringsdokument-for-arbeidet-med-samfunns-sikkerhet-og-beredskap-i-kunnskapssektoren/id2512037/

Beredskapsrådets veileder for gjennomføring av risiko- og sårbarhetsanalyser
Veileder i risiko- og sårbarhetsanalyser for kunnskapssektoren | Universitetet i Stavanger

CESAER: *Input Note on Research security as a collective responsibility: empowering universities, enabling Europe*
https://www.cesaer.org/content/5-operations/2025/20251027-cesaer-input-note-research-security.pdf

Direktoratet for høyere utdanning og kompetanse (HK-dir): *Retningslinjer og verktøy for ansvarlig internasjonalt kunnskapssamarbeid*
Retningslinjer og verktøy for ansvarlig internasjonalt kunnskapssamarbeid | HK-dir

Direktoratet for høyere utdanning og kompetanse (HK-dir): *Geopolitisk spenning og internasjonalt kunnskapssamarbeid – en kvalitativ studie av erfaringer i norske fagmiljø*
Geopolitisk spenning og internasjonalt kunnskapssamarbeid | HK-dir

FFI: *Hva vet vi om innsiderisiko*
https://www.ffi.no/aktuelt/blogg/vi-ma-prioritere-personellsikkerhet

Finans Norge: *Veileder i personellsikkerhet for finansnæringen*
Veileder i personellsikkerhet for finansnæringen

Forskningsrådet: Fire anbefalinger for et helhetlig forskningssystem for åpen, skjermet og gradert forskning
Fire anbefalinger for et helhetlig forskningssystem for åpen, skjermet og gradert forskning

NSM*: Grunnprinsipper for personellsikkerhet*
Grunnprinsipper for personellsikkerhet .pdf

NSM: *Temarapport Innsidere*
Temarapport innsidere.pdf

Næringslivets Sikkerhetsråd: Veileder til personellsikkerhet
Personellsikkerhet-Kort-veileder.pdf

Næringslivets Sikkerhetsråd: *Sårbarhetssamtaler*
https://www.nsr-org.no/uploads/documents/Publikasjoner/Veileder-i-sarbarhetssamtaler.pdf

PST, NSM, Politiet og Næringslivets Sikkerhetsråd: *Sikkerhet ved ansettelsesforhold*
https://nsm.no/aktuelt/ny-veileder-sikkerhet-ved-ansettelsesforhold

SINTEF: En metastudie om innsidetrusselen
En metastudie om innsidetrusselen - SINTEF

SINTEF: Navn
Kunnskapsgrunnlag om bevisstgjøringsstrategier som skal motvirke rekruttering av ubevisste innsidere i norske virksomheter - SINTEF

Statnett: *Veileder i personellsikkerhet for kraftforsyningen*
https://publikasjoner.nve.no/veileder/2024/veileder2024_01.pdf

Saker behandlet av *Diskrimineringsnemda*
https://www.diskrimineringsnemnda.no/