

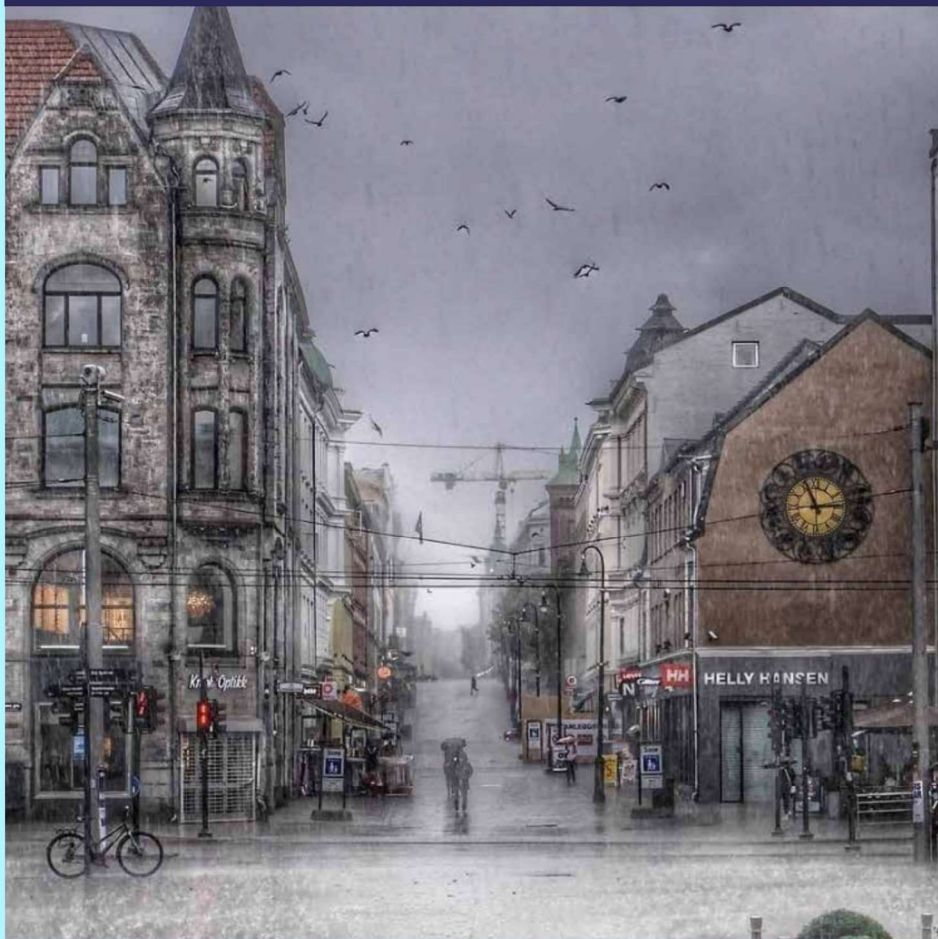


Oslo

Beredskapsetaten

Del 6: Sikkerhetsklarering og autorisasjon

Veileder i helhetlig og systematisk
arbeid med samfunnssikkerhet og
beredskap



Nøkkelord: Informasjonssikkerhet, personellsikkerhet, skjermingsverdig, sikkerhetsgradert, sikkerhetsklarering, autorisasjon			Distribusjon: Alle virksomheter i Oslo kommune.	
			Referanse til deler eller utdrag av denne veilederen som kan føre til feiltolkning, er ikke tillatt.	
Rev. nr.	Dato	Endringer ved revisjon	Utarbeidet av	Godkjent av
1.0	30.09.2019	Veileder etablert	Ivar Wiig	Sverre Martin Bakkeli
2.0	10.01.2023	Endret layout iht. gjeldene retningslinjer for Oslo kommune. Lagt til tabellen med revisjonsinformasjon.	Giulia Caruso	Sverre Martin Bakkeli
		Gjennomgang og oppdatering	Lotte Oddaker	

Innhold

1	Innledning.....	1
2	Hjemmelsgrunnlag – lov og forskrift.....	2
2.1	Sikkerhetslovgivningen.....	2
2.2	Informasjonssikkerhet.....	2
2.2.1	Verdivurdering av informasjon	2
2.2.2	Sikkerhetsgradering av informasjon.....	3
2.3	Personellsikkerhet.....	3
2.3.1	Sikkerhetsklarering	4
2.3.2	Autorisasjon	5
2.4	Bortfall, tilbakekallelse, nedsettelse og suspensjon av sikkerhetsklarering og autorisasjon	7
2.5	Oppbevaring av sikkerhetskonnvolutt.....	7
3	Ansvarsforhold i Oslo kommune.....	8
4	Flytskjema sikkerhetsklarering og autorisasjon	10
	Begrep.....	11

1 Innledning

Denne veilederen forklarer hvordan Oslo kommune overholder Sikkerhetsloven¹ gjennom å styre hvem som får tilgang til sikkerhetsgradert informasjon. Veilederen forklarer hva Sikkerhetsloven betyr for kommunen på dette området, hvordan ansvaret er fordelt innad i kommunen, og hvordan prosessen for å gis tilgang til sikkerhetsgradert informasjon skal gjennomføres.

Sikkerhetsgradert informasjon er informasjon som kan skade nasjonale sikkerhetsinteresser dersom den blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.²

Enkelte ansatte i Oslo kommune har arbeidsoppgaver som gjør at de har behov for å jobbe med sikkerhetsgradert informasjon. Dette kan for eksempel være i forbindelse med jobb på skjermingsverdig objekt, infrastruktur eller informasjonssystem, eller i arbeid med saker knyttet til disse. Ansatte i ulike leder-, sikkerhets-, eller beredskapsstillinger kan ha behov for tilgang på sikkerhetsgradert informasjon i arbeidet med beredskapsplanlegging eller i en krisehåndteringssituasjon.

For å få tilgang til sikkerhetsgradert informasjon må en person ha et tjenstlig behov for det. For tilgang på informasjon sikkerhetsgradert på nivå BEGRENSET kreves kun autorisasjon. For gradert informasjon på nivå KONFIDENSIELT og høyere må personen være både sikkerhetsklarert og autorisert for å kunne bli gitt tilgang.

Selv om en er autorisert for HEMMELIG, betyr ikke det at en er godkjent for tilgang til all sikkerhetsgradert informasjon opp til og med dette nivået. «Need to know»-prinsippet gjelder. En skal kun gis tilgang til den informasjonen som en har tjenstlig behov for.

Alle som får tilgang til sikkerhetsgradert informasjon som ledd i arbeid eller tjeneste for en virksomhet, har taushetsplikt om innholdet. Taushetsplikten gjelder også etter at arbeidet eller tjenesten er avsluttet.

Håndteringen av sikkerhetsgradert informasjon, altså tilvirkning, merking, lagring, distribusjon og bruk m.v., reguleres i Sikkerhetsloven og virksomhetsikkerhetsforskriften.

¹ Lov om nasjonal sikkerhet LOV-2018-06-01-24

² Sikkerhetsloven §5-1

2 Hjemmelsgrunnlag – lov og forskrift

2.1 Sikkerhetslovgivningen

Ny Sikkerhetslov ble gjeldende fra og med 1.januar 2019. Lovens formål er:

- å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser
- å forebygge, avdekke og motvirke sikkerhetstruende virksomhet
- at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

Til loven hører blant annet «Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften)³» og «Forskrift om sikkerhetsklarering og annen klarering (klareringsforskriften)⁴».

2.2 Informasjonssikkerhet⁵

Med informasjonssikkerhet menes å sikre konfidensialiteten, integriteten og tilgjengeligheten til alle former for informasjon en virksomhet benytter som del av å utføre sine oppgaver og levere sine tjenester.

2.2.1 Verdivurdering av informasjon

Verdivurdering av informasjon er en kartlegging og rangering av en virksomhets informasjonsverdier. Det vurderes hvilke konsekvenser det kan gi, både for virksomheten selv og for andre som er avhengige av informasjonen, dersom informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.

Dersom verdivurderingen viser at informasjonen har betydning for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser, er informasjonen skjermingsverdig. Skjermingsverdig informasjon skal beskyttes. Beskyttelsen skal gi et forsvarlig sikkerhetsnivå utfra skadepotensialet knyttet til informasjonens konfidensialitet, integritet og tilgjengelighet.

Det er den virksomheten som eier skjermingsverdig informasjon som må vurdere informasjonens verdi og skadepotensiale. Det er her viktig å fremheve at når en slik vurdering gjennomføres bør dette gjøres av personer som innehar gyldig sikkerhetsklarering og autorisasjon tilsvarende høyeste nivå som informasjonen kan komme til å bli gradert til.

³ FOR-2018-12-20-2053

⁴ FOR-2018-12-20-2054

⁵ Sikkerhetsloven Kapittel 5; Virksomhetsikkerhetsforskriften Kapittel 4, 5 og 6

For mer utfyllende forklaring av verdivurdering henvises det til NSM sin «Veiledning i verdivurdering av informasjon» og «Håndbok i verdivurdering av informasjon» som er tilgjengelig på NSM sine nettsider.⁶

2.2.2 Sikkerhetsgradering av informasjon⁷

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

Når informasjon må beskyttes av konfidensialitetshensyn, skal en av følgende sikkerhetsgrader benyttes:

- STRENGT HEMMELIG nyttes dersom det kan få helt avgjørende skadefølger for nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende
- HEMMELIG nyttes dersom det alvorlig kan skade nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende
- KONFIDENSIELT nyttes dersom det kan skade nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende
- BEGRENSET nyttes dersom det i noen grad kan medføre skadefølger nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.

Det er den som utsteder eller på annen måte tilvirker skjermingsverdig informasjon, som skal sørge for at informasjonen merkes med riktig sikkerhetsgrad i samsvar med sikkerhetslovgivningen.

Sikkerhetsgradering skal ikke skje i større utstrekning enn strengt nødvendig, og det skal ikke brukes høyere sikkerhetsgrad enn det som gir forsvarlig beskyttelse av informasjonen.

2.3 Personellsikkerhet⁸

Med personellsikkerhet menes vurderinger og tiltak som har til hensikt å hindre personer som kan utgjøre en sikkerhetsrisiko å bli eller være plassert i stillinger eller

⁶ <https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/>

⁷ Sikkerhetsloven § 5-3 og virksomhetsikkerhetsforskriften kapittel 5.

⁸ Sikkerhetsloven kapittel 8 og Virksomhetsikkerhetsforskriften kapittel 12

roller som medfører brudd på sikkerhetslovgivningen. Autorisasjon og sikkerhetsklarering inngår i personellsikkerhet og sikkerhetsstyring.

Sikkerhetsgradert informasjon som behandles av kommunens ansatte vil ofte være på nivå BEGRENSET. For tilgang på informasjon gradert på dette nivået behøves kun autorisasjon.

Enkelte ansatte kan ha behov for å behandle informasjon på høyere graderingsnivå, til og med HEMMELIG. Kommunens ansatte vil normalt ikke ha behov for klarering på nivå STRENGT HEMMELIG. For alle som skal ha tilgang til gradert informasjon på nivå KONFIDENSIELT eller høyere, må sikkerhetsklarering være innvilget før autorisering.

Merk at behandling av informasjon merket «unntatt offentlighet» er regulert av Offentleglova⁹, ikke Sikkerhetsloven. En person trenger verken sikkerhetsklarering eller autorisasjon for å behandle slik informasjon. «Need-to-know»-prinsippet gjelder derimot også her; en person skal ikke gis tilgang til informasjon en ikke har tjenstlig behov for.

2.3.1 Sikkerhetsklarering¹⁰

For å bli sikkerhetsklarert for nivå KONFIDENSIELT eller høyere, må det gjennomføres en personkontroll. Vedkommende som skal sikkerhetsklareres må fylle ut en personopplysningsblankett (POB). Dess høyere graderingsnivå en skal gis tilgang til, dess mer omfattende gjøres personkontrollen og mer informasjon må fylles ut i blanketten.

Når vedkommende signerer POB, gir hen samtidig sitt samtykke til at det gjennomføres en personkontroll. Dette inkluderer innhenting av personopplysninger fra ulike databaser tilgjengelig for Sivil Klareringsmyndighet.

Når en søker om sikkerhetsklarering må det angis hvor mange år en søker om å bli klarert for. En kan klareres for opptil fem år av gangen. Her må det gjøres en vurdering på hvor lenge en forventer at den ansatte kommer til å ha behov for tilgang til den graderte informasjonen. En skal ikke søke om klarering for lengre gyldighetstid enn nødvendig.

Det er Sivil Klareringsmyndighet som er klareringsmyndighet for Oslo kommune, mens Beredskapsetaten er kommunens anmodende virksomhet. Det vil si at det bare er Beredskapsetaten som kan anmode Sivil Klareringsmyndighet om å få gjennomført en

⁹ LOV-2006-05-19-16

¹⁰ Sikkerhetsloven § 8-2 Sikkerhetsklarering, § 8-4 Avgjørelse om klarering, § 8-5 Gjennomføring av personkontroll

klareringsprosess (unntaket i Oslo kommune er Vann- og avløpsetaten¹¹ som har fått dispensasjon for å søke direkte til Sivil Klareringsmyndighet).

Når en personopplysningsblankett er ferdig utfyllt skal den og innholdet merkes med PERSONKONTROLL. Det betyr at den må oppbevares på godkjent måte i henhold til Sikkerhetsloven. Informasjon merket PERSONKONTROLL skal oppbevares adskilt fra andre opplysninger i virksomheten, og på en slik måte at bare utpekt personell har tilgang til den.¹²

POB og veiledning til utfylling av denne ligger på NSM sine nettsider.¹³

2.3.1.1 Reklarerer

Om en har behov for fortsatt å være sikkerhetsklarert etter at inneværende klareringen utløper, må en i god tid (ca. seks måneder) før utløp søke om en reklarerer. Dette gjøres ved at en kontrollerer at opplysningene i personopplysningsblanketten fortsatt stemmer, gjør nødvendige endringer, og signerer på punktet «reklarerer». Anmodende myndighet må i tillegg fylle ut et reklareringsvedlegg som sendes inn sammen med personopplysningsblanketten.

2.3.2 Autorisasjon

For at en person skal kunne gis tilgang til sikkerhetsgradert informasjon som del av sin tjeneste hos en virksomhet, må personen ha gjennomført en autorisasjonssamtale med autorisasjonsansvarlig i virksomheten. Vilkår for å autorisere er at autorisasjonsansvarlig selv er sikkerhetsklarert og autorisert samt formelt har fått delegert autorisasjonsansvaret.

I byrådssak 1029/19 har Byrådet delegert autorisasjonsansvaret i Oslo kommune til den enkelte byråd. Hver byråd har autorisasjonsansvar innenfor sin sektor. Dette ansvaret kan delegeres videre innenfor sektoren. Det er naturlig at byråden delegerer dette ansvaret til kommunaldirektør i egen byrådsavdeling. Dersom virksomheter under byrådsavdelingen har et stort autorisasjonsbehov, kan autorisasjonsansvaret delegeres til virksomhetsleder. Virksomhetsleder kan videre delegere ansvaret til for eksempel sikkerhetsleder dersom virksomheten har dette.

Før autorisasjonssamtale kan gjennomføres må det signeres en taushetserklæring¹⁴¹⁵. Gjennom autorisasjonsavtalen skal autorisasjonsansvarlig sjekke at den som skal autoriseres har tilstrekkelig kunnskap om og forståelse av trusselbilde,

¹¹ Vann- og avløpsetaten er fra 2017 anmodende myndighet for sine egne ansatte og andre som jobber med prosjekter for etaten. Beredskapsetaten er anmodende virksomhet for alle andre i kommunen.

¹² Virksomhetsikkerhetsforskriften § 76 og § 77

¹³ <https://nsm.no/regelverk-og-hjelp/skjemaer/>

¹⁴ Virksomhetsikkerhetsforskriften § 67

¹⁵ <https://nsm.stat.no/globalassets/dokumenter/skjemaer/taushetserklaring-nbnn-0119.pdf>

skjermingsverdige verdier og sikkerhetsbestemmelser, og innhente og kontrollere nødvendige opplysninger om den som skal autoriseres.

Autorisasjonsansvarlig skal vurdere om vedkommende er sikkerhetsmessig skikket og kan utvises tillit til å håndtere sikkerhetsgradert informasjon på angitt nivå. Autorisasjon kan bare gis dersom autorisasjonsansvarlig ikke har opplysninger som gjør det tvilsomt om vedkommende sikkerhetsmessig er til å stole på.

Når autorisasjon er utført, skal autorisasjonsansvarlig fylle ut et autorisasjonsbevis samt signere for gjennomført autorisasjonssamtale på sikkerhetskonvolutten. Autorisasjonsbeviset legges i sikkerhetskonvolutt sammen taushetserklæring og eventuelt klareringsbevis og personopplysningsblankett (POB).

Sikkerhetskonvolutten med innhold er sikkerhetsgradert informasjon og personsensitiv informasjon som skal oppbevares i henhold til bestemmelser for dette, se kapittel 2.5.

2.3.2.1 Tilgang uten autorisasjon¹⁶

Dersom vilkårene i straffelovens § 17 om nødrett er oppfylt (akutt fare for liv og helse eller tap av store økonomiske verdier), kan en person autoriseres uten å inneha nødvendig sikkerhetsklarering, dersom det ikke foreligger rimelig tvil om vedkommendes pålitelighet, lojalitet eller sunne dømmekraft.

Dette er imidlertid ikke en vanlig praksis og skal kun benyttes i ekstreme tilfeller der en persons innsikt i den graderte informasjonen er nødvendig for å forhindre et større negativt utfall i de nevnte kategoriene (liv og helse eller økonomiske verdier). En virksomhet som gir en slik tilgang skal, via autorisasjonsansvarlig, uten ugrunnet opphold varsle klareringsmyndigheten og NSM om hvilke personer som ble gitt tilgang, og på hvilket nivå.

2.3.2.2 Autorisasjon av leverandører

Dersom leverandør av varer og tjenester til Oslo kommune kan komme i besittelse av gradert informasjon, må leverandøren og personellet være autorisert. Det er den kommunale virksomheten som er oppdragsgiver og eier av den graderte informasjonen, som skal autorisere disse. Dersom graderingsnivået er over BEGRENSET, må personellet hos leverandør også ha gyldig sikkerhetsklarering på det graderingsnivået de skal autoriseres for.

Det anbefales at behovet for autorisasjon og eventuelt sikkerhetsklarering avklares før anskaffelsen legges ut på anbud, da et eventuelt krav om autorisasjon og sikkerhetsklarering av personell hos tilbydere bør fremgå av utlysning dokumentene.

¹⁶ Virksomhetsikkerhetsforskriften § 71

2.4 Bortfall, tilbakekallelse, nedsettelse og suspensjon av sikkerhetsklarering og autorisasjon¹⁷

Sikkerhetsklarert og autorisert personell skal holde autorisasjonsansvarlig orientert om forhold som antas å kunne være av betydning for vedkommendes sikkerhetsmessige skikkethet.

Fremkommer det opplysninger som reiser tvil om en sikkerhetsklarert persons sikkerhetsmessige skikkethet, skal klareringsmyndigheten vurdere å tilbakekalle eller nedsette klareringen, eller suspendere klareringen, og iverksette nærmere undersøkelser for å avklare forholdet.

Er en sikkerhetsklarering besluttet tilbakekalt, nedsatt eller suspendert fra klareringsmyndighetens side, skal en begrunnet melding om dette sendes til Nasjonal sikkerhetsmyndighet, og autorisasjonsansvarlig skal varsles umiddelbart.

Autorisasjon bortfaller automatisk når:

- personen fratrer den stilling som autorisasjonen omfatter,
- behovet for autorisasjon av andre grunner ikke lenger er til stede, eller
- vedkommende ikke lenger har tilstrekkelig sikkerhetsklarering

Får autorisasjonsansvarlig opplysninger som gir grunn til tvil om en autorisert person fortsatt kan anses sikkerhetsmessig skikket, skal autorisasjonen vurderes tilbakekalt, nedsatt eller suspendert. Avgjørelse om dette skal meldes til klareringsmyndigheten.

Dersom en autorisasjon skal endres eller tilbakekalles skal vurderingen og avgjørelsen dokumenteres.

Når autorisasjon bortfaller skal autorisasjonsbeviset tilintetgjøres.

2.5 Oppbevaring av sikkerhetskonvolutt

Alle som autoriseres skal ha en egen sikkerhetskonvolutt der all sikkerhetsinformasjon om vedkommende samles. En sikkerhetskonvolutt er en spesiell type konvolutt øremerket til dette formålet. Virksomhetene kan henvende seg til Beredskapsetaten for å få tilsendt slike etter behov.

¹⁷ Sikkerhetsloven § 8-8 og § 8-10. Virksomhetsikkerhetsforskriften § 74

[illegible]

Når en person er autorisert skal sikkerhetskonvolutten inneholde autorisasjonsbevis og taushetserklæring og eventuelt klareringsbevis og personopplysningsblankett. Konvolutten merkes med sikkerhetsgradering BEGRENSET. Konvolutten oppbevares hos den kommunale virksomheten som gjennomfører autorisasjon (byrådsavdeling eller virksomhet). Når en sikkerhetskonvolutt inneholder en ferdig utfylt personopplysningsblankett, må den merkes

med PERSONKONTROLL.

Dersom en ansatt som er sikkerhetsklarert bytter jobb til annen virksomhet i eller utenfor Oslo kommune, og fortsatt har behov for sikkerhetsklarering i sin nye jobb, skal sikkerhetskonvolutten med innhold oversendes autorisasjonsansvarlig ved nytt tjenestested. Når virksomheter utveksler opplysninger merket PERSONKONTROLL og BEGRENSET skal det gjøres på en slik måte at ingen uvedkommende får tilgang til opplysningene.

3 Ansvarsforhold i Oslo kommune

Med utgangspunkt i bystyresak 182/16 av dato 22.06.2016 og byrådssak 1029/19 av dato 19.03.2019, settes følgende ansvarsforhold for autorisasjonsmyndighet i Oslo kommune:

Byrådene:

- Skal sikkerhetsklareres av Sentral Klareringsmyndighet
- skal autoriseres av beredskapsleder hos Statsforvalteren i Oslo og Viken (STOV)
- skal delegere autorisasjonsmyndighet til kommunaldirektør

Kommunaldirektørene:

- skal sikkerhetsklareres av Sentral Klareringsmyndighet
- skal autoriseres av egen byråd (alternativt kan dette gjøres av Beredskapsetaten på forespørsel)
- får videredelegert autorisasjonsmyndighet fra egen byråd
- vurderer behov for sikkerhetsklarering av personell i egen og underliggende virksomheter

- autoriserer ansatte i egen virksomhet og virksomhetsledere i egen sektor der det vurderes at det er behov for dette (alternativt kan dette gjøres av Beredskapsetaten på forespørsel)
- delegerer autorisasjonsmyndighet til seksjonssjefer i byrådsavdelingen og til virksomhetsledere i sektor dersom det vurderes som hensiktsmessig (fortrinnsvis fordi disse har flere ansatte og eventuelt innleide i egen organisasjon som skal autoriseres)
- er ansvarlig for at byrådsavdelingen til enhver tid har oversikt over egne ansatte og innleide som er autorisert, og anmoder Beredskapsetaten om reklarering i god tid før inneværende klarering utløper

Seksjonssjefer i byrådsavdelingene og virksomhetsledere (dersom det er vurdert behov):

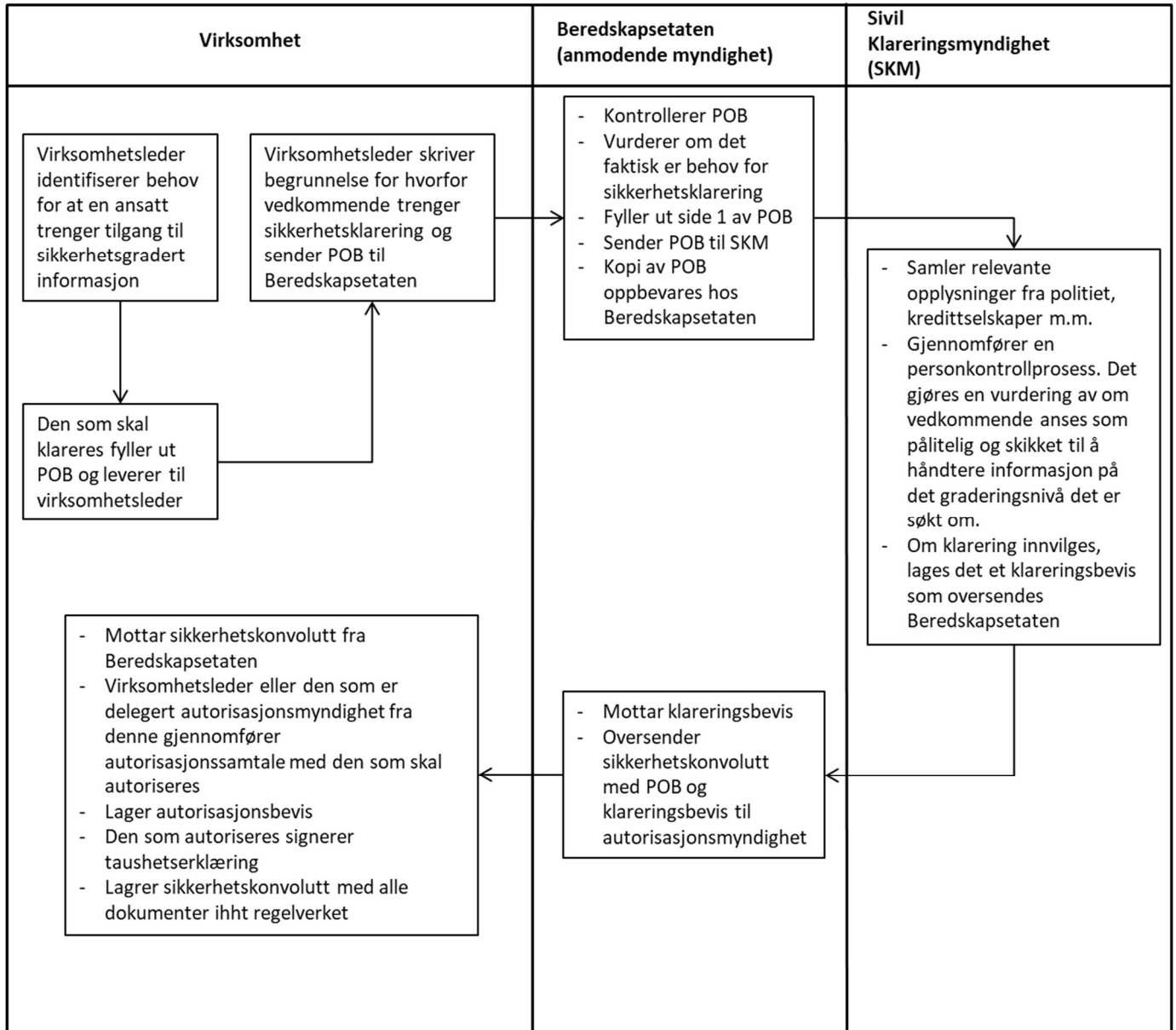
- skal sikkerhetsklareres av Sentral Klareringsmyndighet
- skal autoriseres av kommunaldirektør
- skal vurdere behov for sikkerhetsklarering og autorisering av egne ansatte og innleide, herunder vurdere for hvilket graderingsnivå det er behov for å sikkerhetsklarere og autorisere på
 - o Beredskapsetaten anbefaler at virksomheter som kan få en rolle i en krisehåndteringssituasjon, som et minimum sikkerhetsklareres og autoriserer virksomhetsleder, stedfortredende virksomhetsleder, beredskapsansvarlig og sikkerhetsleder (om en har dette).
- kan delegere autorisasjonsmyndigheten videre til eksempelvis sikkerhetsleder
- er ansvarlig for oppbevaring av informasjon om de ansattes autorisasjon og sikkerhetsklarering (sikkerhetskonvolutt)
- er ansvarlig for at virksomheten til enhver tid har oversikt over egne ansatte og innleide som er autorisert, og anmoder Beredskapsetaten om reklarering i god tid før inneværende klarering utløper

Beredskapsetaten:

- er anmodende virksomhet på vegne av Oslo kommune
 - o mottar klareringssøknader fra øvrige kommunale virksomheter (med unntak av Vann- og avløpsetaten som gjør dette selv) og fremsender disse til behandling hos Sivil klareringsmyndighet (SKM)
 - o videreformidler SKM sin beslutning til den som har søkt om klarering
- Gir veiledning i prosess for sikkerhetsklarering og autorisasjon, og gir opplæring til kommunens virksomheter i hvordan de skal gå frem for å gjennomføre autorisasjon

- følger opp at byrådene klareres og autoriseres, samt reklarerer i god tid før klareringen utløper. Beredskapsetaten holder ikke oversikt over andre ansattes klareringsstatus.

4 Flytskjema sikkerhetsklarering og autorisasjon



Skjemaet viser saksgangen fra det identifiseres behov for å sikkerhetsklarere og autorisere en ansatt og frem til autorisasjonssamtalen er gjennomført.

Begrep

Begrep	Forklaring
Anmodende myndighet	Et forvaltningsorgan som i egenskap av eller på vegne av autorisasjonsansvarlig anmoder om personkontroll. Beredskapsetaten er anmodende myndighet på vegne av Oslo kommune (Vann- og avløpsetaten er anmodende myndighet for egen virksomhet).
Autorisasjon	Avgjørelse, foretatt av autorisasjonsansvarlig, om at en person etter forutgående, bedømmelse av kunnskap om sikkerhetsbestemmelser, tjenstlig behov samt avlagt skriftlig taushetsløfte, samt eventuell sikkerhetsklarering, gis tilgang til informasjon med angitt sikkerhetsgrad.
Autorisasjonsansvarlig	Ansvarlig for autorisasjon av ansatte som skal gis tilgang til sikkerhetsgradert informasjon. Virksomhetsleder eller den som har blitt delegert denne myndigheten.
Informasjonssikkerhet	Tiltak for beskyttelse av informasjonsverdier etter konfidensialitet, integritet og tilgjengelighet
Klareringsmyndighet	Myndighet som gjennomfører personkontroll og vurderer om en person kan gis sikkerhetsklarering eller ikke. Sivil klareringsmyndighet (SKM) er klareringsmyndighet for Oslo kommune.
Personkontroll	Innhenting og vurdering av relevante opplysninger i forbindelse med vurdering av sikkerhetsklarering.
Personopplysningsblankett (POB)	Blankett for utfylling av personopplysninger. Brukes i forbindelse med personkontroll til sikkerhetsklarering.
Personellsikkerhet	Tiltak, handlinger og vurderinger for å hindre at personer som vil kunne utgjøre en sikkerhetsrisiko, plasseres eller er plassert slik at risikoen aktualiseres.
Sikkerhetsgradert informasjon	Skjermingsverdig informasjon som skal beskyttes av konfidensialitetshensyn, og er merket med sikkerhetsgrad etter reglene i Sikkerhetslovens § 5-3.
Sikkerhetsklarering	Avgjørelse, foretatt av klareringsmyndighet og bygget på personkontroll, om en persons antatte sikkerhetsmessige skikkethet for angitt sikkerhetsgrad.
Sikkerhetskonnolutt	Spesiell type konvolutt for oppbevaring av alle relevante opplysninger knyttet til en persons

	sikkerhetsklarering og autorisasjon. Dette er blant annet personopplysningsblankett, klareringsbevis, autorisasjonsbevis og taushetserklæring. Konvolutten kan bestilles fra Beredskapsetaten.
Skjermingsverdig informasjon	Informasjon som må beskyttes fordi den, om den blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig, kan skade nasjonale sikkerhetsinteresser.
Taushetserklæring	Skjema der en person erklærer at den er kjent med hvilke plikter som medføres ved å få tilgang til taushetsbelagt informasjon.