i Arbeids- og velferdsetaten

(Informasjonssikkerhetspolicy)

«Dette er det overordnede styringsdokumentet i Arbeids- og velferdsetatens internkontrollsystem for personvern, informasjonssikkerhet og beredskap. Dokumentet beskriver rammer, mål, myndighet og ansvar som ligger til grunn for sikkerhetsarbeidet i etaten.»

Godkjent 16.02.2018

ENDRINGSLOGG

Ver.	Dato	Kap.	Endring	Produsent	Godkjent av
1.0	16.08.2006	Alle	Fremleggelse for Arbeids- og velferdsdirektør	Sikkerhetsledelsen	Tor Saglie
2.0	28.04.2010	Alle	Fremleggelse for IKT-direktør	IT-sikkerhetsansvarlig	Nina Aulie
2.0.4	30.10.2012	Alle	Ingen	Seksjon PIB	D-møte
2.1.0	04.02.2015	Alle	Oppdatert etter omorganisering og koplet til virksomhetsstrategien	Sikkerhetsseksjonen	
2.1.1	17.02.2015	Alle	Ingen	Sikkerhetsseksjonen	D-møte
2.1.8	27.06.2017	Alle	Sendt på høring i avdelingene	Sikkerhetsseksjonen	
2.1.9	01.09.2017	Alle	Innarbeidelse av høringssvar	Sikkerhetsseksjonen	
2.2	16.02.2018	Alle	Gjeldende fram til mai 2018	Sikkerhetsseksjonen	Geir Axelsen

INNHOLDSFORTEGNELSE

1. SIKKERHET ER VIKTIG FOR DEG

Som arbeids- og velferdsdirektør har jeg det overordnede ansvaret for sikkerheten i etaten og skal sørge for at NAV behandler informasjon i henhold til gjeldende lover og forskrifter.

Dette styringsdokumentet beskriver overordnede prinsipper og krav til sikkerhet i Arbeids- og velferdsetaten. Alle medarbeidere må gjøre seg kjent med de sikkerhetskrav som gjelder.

Personopplysningsloven legger mange føringer for arbeidet med informasjonssikkerhet. Brukernes og samfunnets tillit til NAV er tuftet på at alle de vi samhandler med kan føle seg trygge på at vi alltid vil bestrebe oss på å behandle personopplysninger på en respektfull og sikker måte. Alle medarbeidere skal overholde taushetsplikten og all bruk av fagsystemene skal være knyttet til tjenstlig behov. Brudd på sikkerhetsreglene skal alltid følges opp av nærmeste leder og vil i alvorlige tilfeller medføre tjenstlige reaksjoner eller politianmeldelse.

Det skal være trygt å arbeide i NAV. Vi aksepterer ikke at medarbeidere utsettes for vold eller trusler om vold i kontakt med enkeltbrukere. Dessverre skjer det likevel slike hendelser. Hvordan vi håndterer trusselsituasjoner som oppstår, og hvilke tiltak vi planlegger og gjennomfører for å unngå slike hendelser, skal være en sentral del av vårt beredskapsarbeid. Det skal øves på dette på lik linje med planene for kontinuitet i driften av våre IT-systemer som sikrer livsoppholdsytelser til befolkningen.

God sikkerhet bidrar til verdiskaping og til godt omdømme for etaten, noe som vil gi seg utslag i økt tilfredshet blant brukere, samarbeidspartnere og medarbeidere. Det er vårt ansvar å vise at vi tar sikkerhet på alvor.

Hilsen

Sigrun Vågeng
Arbeids- og velferdsdirektør

Fra våren 2018 etableres et eget styringssystem for personvern som vi oveta for de delene i dette styringssystemet som omhandler personvern. Dette styringsdokument vil bli oppdatert i etterkant av at et nytt styringssystem for personvern trer i kraft.

2. STYRINGSSYSTEMETS OPPBYGGING

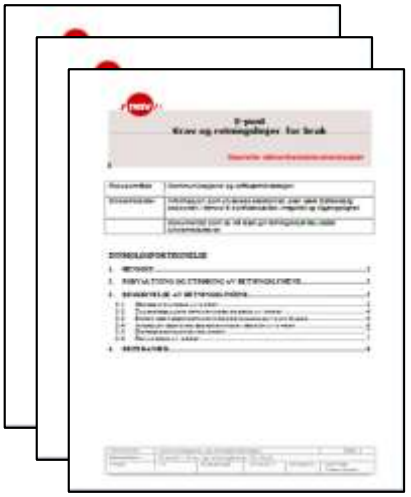
I dette styringsdokumentet benyttes begrepet sikkerhet både om personvern, informasjonssikkerhet og beredskap.

Etatens styringssystem bygger på standarden NS ISO/IEC 27001:2013 'Informasjonsteknologi – Sikringsteknikker – Ledelsessystemer for informasjonssikkerhet – Krav', og er i tråd med anbefalingene fra Difi (Direktoratet for forvaltning og IKT). Styringssystemet består av to dokumenter:

Styringsdokument for personvern, informasjonssikkerhet og beredskap inneholder rammer, mål, myndighet og ansvar for sikkerhetsarbeidet i etaten.

Overordnede sikkerhetskrav inneholder etatens sikkerhetskrav inndelt i 15 fokusområder.

I tillegg er det utviklet et sett med operative retningslinjer innenfor de 15 fokusområdene. Dette er detaljerte retningslinjer med veiledninger som er å finne på Navet under hurtigvalget 'Gå direkte til', velg deretter menypunktet Personvern, informasjonssikkerhet og beredskap.



3. MÅL FOR SIKKERHET

Sikkerhetstiltak skal bidra til å realisere virksomhetsmålene uten å virke hindrende for virksomhetens behov.

Figur 2: *Sikkerhet knyttet til etatens virksomhetsmål*

Bedre brukermøter: Vi sikrer informasjonen i NAV for at brukerne skal ha tillit til å gi oss den informasjonen vi trenger for å gi brukeren korrekte ytelser og tjenester. Vi må sørge for at selvbetjeningsløsningene er slik at etatens aktive brukere kan bruke dem på en sikker og brukervennlig måte.

Økt kompetanse: For å oppnå dette må sikkerhetsregimet i NAV være slik at medarbeiderne kan etterleve de kravene som blir stilt i det daglige arbeidet. Dette krever at nødvendige sikringstiltak er enkle å gjennomføre og at medarbeiderne får kompetanse til å gjøre sine oppgaver på en sikker måte.

På denne måten er etterlevelse av lover, virksomhetsstrategi og langtidsplan førende for sikkerhetsmålene i NAV.

Godt personvern har vi

- når brukerne stoler på at NAV behandler personopplysninger på en sikker måte
- når brukerne stoler på at NAV overholder taushetsplikten
- når all bruk av fagsystemene er knyttet til tjenstlig behov
- når brukerne får informasjon og innsyn i sine opplysninger
- når brukerne får rettet feil personopplysninger

God informasjonssikkerhet er

- å sikre at informasjonen ikke blir kjent for uvedkommende (konfidensialitet)
- å sikre at informasjonen ikke blir endret utilsiktet eller av uvedkommende (integritet)
- å sikre at informasjon og systemer er tilgjengelig ved behov (tilgjengelighet)
- å sikre sporbarhet for behandling av informasjon

God beredskap er

- å sikre at NAV kan utføre sine kritiske tjenester ved unormale og alvorlige hendelser som rammer samfunnet
- å sikre kontinuitet slik at IT-systemene fungerer ved driftsmessige forstyrrelser eller svikt i levering av strøm, datanettverk, telefoni eller betalingstjenester
- å trygge medarbeidernes arbeidssituasjon ved å redusere risikoen for vold og trusler om vold
- å sørge for at NAV er godt nok forberedt på å håndtere uønskede hendelser slik at vi raskt kan gjenopprette en normal driftssituasjon

4. STRATEGI

De langsiktige og overordnede prioriteringene for NAV ligger fast: Flere i arbeid, bedre brukermøter og økt kompetanse.

4.1 Prinsipper i sikkerhetsarbeidet

- **Tjenstlig behov**. Etatens medarbeidere skal kun ha tilgang til systemer, informasjon, omgivelser og lokaler som medarbeideren har behov for i arbeidet sitt og kun for den tiden behovet er der
- **Ansvarsprinsipp**. Den som har ansvar for forvaltning, drift eller bruk av IT-utstyr, systemer, data eller andre ressurser, er ansvarlig for sikkerheten ved forvaltning, drift eller bruk
- **Innebygd personvern**. Vi utvikler systemer og prosesser etter prinsipper for innebygd personvern («Privacy by design»)
- **Arbeidsdelingsprinsipp**. Oppgaver som det innebærer for stor risiko at én medarbeider løser alene, løses ved at to medarbeidere gjør hver sin del
- **Et integrert sikkerhetsregime**. Ved utvikling av sikkerhetsregler og -retningslinjer skal det sikres medvirkning fra de som blir berørt. Alle operative retningslinjer og øvrig informasjons- og veiledningsmateriell skal ha klart definerte målgrupper og ha et klart og tydelig språk. Der det er mulig skal krav og operative retningslinjer knyttet til sikkerhetsarbeid integreres i øvrige prosessbeskrivelser og retningslinjer for å sikre en mest mulig helhetlig oversikt for de som skal forholde seg til disse.

4.2 Effekt av sikkerhetstiltak og sikkerhetsprosjekter

Prosjekter og enkelttiltak som skal føre til bedre sikkerhet for NAV, må synliggjøre at de gir slik effekt. Effekten kan komme ved å gjøre eksisterende sikkerhetstiltak mer effektive, å sette organisasjonen i stand til å gjøre nye ting og å utbedre manglende sikkerhet eller etterlevelse av regler på sikkerhetsområdet.

4.3 Aksept og håndtering av risiko

Risikohåndtering av personvern, informasjonssikkerhet og beredskap inngår i den helhetlige tilnærmingen i NAVs felles metode for risikostyring. Denne angir hva som er akseptabel risiko. Vi klassifiserer informasjon, prosesser og informasjonssystemer for å få kunnskap om hva som er mest kritisk slik at vi på en ensartet måte kan tilpasse sikkerhetstiltakene i forhold til behovet for sikring.

4.4 Oppfølging av hendelser

Et sikkerhetsbrudd kan være en bevisst handling, unnlatelse eller uaktsomhet som bryter med sikkerhetskravene og som fører til skade for brukere, økonomisk tap, tap av tillit, eller er til skade for NAVs ansatte eller virksomheten.

Alle sikkerhetsbrudd, forsøk eller indikasjoner på sikkerhetsbrudd skal meldes til nærmeste leder og registreres i etatens avvikssystem (ASYS). Brudd på etatens sikkerhetskrav følges opp overfor de ansatte. Reaksjonene vil variere avhengig av overtredelsens alvorlighet.

5. ROLLER OG ANSVAR FOR SIKKERHET

De enkeltes ansvar og oppgaver er beskrevet i ansvarsdokument for direktoratet, i mål og disponeringsbrev til enheter og i organisasjonsplaner og rolledokument. I dette kapittelet konkretiserer vi hva dette betyr på sikkerhetsområdet.

5.1 Regimeansvar for sikkerhet

Ansvaret for styringssystemet er lagt til Økonomi- og styringsavdelingen i Arbeids- og velferdsdirektoratet. Det samme gjelder regimeansvaret for informasjonssikkerhet og beredskap. Regimeansvaret for personvern er lagt til Kunnskapsavdelingen

Direktøren i Økonomi- og styringsavdelingen godkjenner dokumentet 'Overordnede sikkerhetskrav' som fastsetter kravene til sikkerhet innenfor rammen av styringsdokumentet og etter føringer fra Kunnskapsavdelingen på personvernområdet. Myndighet for daglig arbeid med sikkerhet er delegert til lederen for sikkerhetsseksjonen, tilsvarende leder for juridisk seksjon når det gjelder personvern.

5.2 Medarbeidere

En medarbeider kan være fast eller midlertidig ansatt, innleid konsulent, renholdsmedarbeider, håndverker eller annen medarbeider som utfører arbeid på oppdrag for etaten. Alle medarbeidere har ansvar for å

- gjøre seg kjent med reglene for taushetsplikt og å undertegne taushetserklæring
- gjøre seg kjent med 'Felles sikkerhetsnormer for Arbeids- og velferdsetaten'og å undertegne 'lokal sikkerhetsinstruks for medarbeider' samt følge påleggene som gis i instruksen
- sette seg inn i og overholde etatens sikkerhetskrav som er relevante for den rollen en har i ulike situasjoner og hva som er akseptabel bruk av informasjon og IT-systemer
- bruke IT-systemene som beskrevet i brukerdokumentasjonen
- melde fra om avvik eller sikkerhetsbrudd eller mistanke om dette i Avvikssystemet (ASYS)

5.3 Ledere

Ansvaret for sikkerheten er et linjeansvar. Alle ledere i NAV skal etablere og opprettholde et tilstrekkelig sikkerhetsnivå innenfor sitt ansvarsområde. Ansvaret kan ikke delegeres, men spesifikke oppgaver kan overlates til en sikkerhetskoordinator, sikkerhetsmedarbeider eller andre medarbeidere.

Dette innebærer at lederen skal

- undertegne 'sikkerhetsinstruks for leder' og påse at sikkerhetsarbeidet ivaretas og er forankret hos medarbeiderne
- sørge for at medarbeidere i enheten har tilstrekkelig kunnskap, bevissthet, holdninger og ferdigheter til å kunne overholde kravene til personvern, informasjonssikkerhet og beredskap.
- utarbeide planer for arbeidet med sikkerhet etter gjennomført risikoanalyse
- sørge for at de som gis sikkerhetsoppgaver har kompetanse og handlingsrom til å utføre disse oppgavene

5.4 Personvernombud

Personvernombudet skal være kontaktpunkt for etatens brukere i saker som har med behandling av personopplysninger å gjøre. I tillegg har personvernombudet som oppgave å øke kunnskap og oppmerksomhet om personvern i etaten, herunder informere og gi råd til etaten og til ansatte i saker som handler om personvern.

Sentrale arbeidsoppgaver er å

- føre oversikt over etatens behandlinger av personopplysninger
- passe på at ledelsen i etaten har etablert et system for internkontroll
- bistå personer som er registrert som brukere av etaten
- besvare spørsmål om personvern internt i etaten
- være rådgiver for den behandlingsansvarlige for personopplysninger
- peke på brudd på personopplysningsloven overfor ledelsen
- være en kontaktperson ved henvendelser fra Datatilsynet
- holde seg orientert om utviklingen innen personvern

5.5 Sikkerhetskoordinator

Sikkerhetskoordinatorer utpekes i avdelingene i direktoratet, fylkeskontorene og i styringsenhetene for å koordinere sikkerhetsarbeidet i egen enhet og underliggende enheter.

Sikkerhetskoordinatorene har sikkerhetsseksjonen i direktoratet som faglig kontaktpunkt og skal bidra til at sikkerhetsarbeidet gjøres så effektivt og virkningsfullt som mulig.

Sikkerhetskoordinatoren kan bistå enhetslederen med å:

- koordinere og yte bistand innen sikkerhetsområdet i egen styringslinje
- påse at egen og underlagte enheter følger planlagte tiltak og pålagte krav
- påse at egen enhets og underlagte enheters sikkerhetsinstruks etterleves, herunder særskilt:
  - gjennomføre risikovurderinger for personvern, informasjonssikkerhet og beredskap
  - bidra i utarbeidelse av lokale sikkerhetsinstrukser og beredskapsplaner
  - utarbeide lokale opplærings- og motivasjonstiltak for personvern, informasjonssikkerhet og beredskap
  - påse at tilganger til applikasjoner, servere og nettverk gis ut fra et tjenstlig behov
  - gjennomgang av sikkerhetslogger og sikkerhetsrapporter
- følge opp at iverksatte sikringstiltak fungerer som forutsatt ved egen og underlagte enheter
- etablere og oppdatere lokale kontinuitets- og beredskapsplaner
- håndtere og følge opp avvik og sikkerhetsbrudd

5.6 Sikkerhetsmedarbeider/Sikkerhetsrådgiver

Enhetsleder kan velge å utpeke en medarbeider til å arbeide med sikkerhet innen egen enhet. Sikkerhetsmedarbeideren vil få sikkerhetskoordinator i egen styringslinje som faglig støtteperson.

5.7 Identadministrator

Enhetsleder er ansvarlig for tildelte tilganger til medarbeiderne i sin enhet. Den praktiske oppgaven med å legge inn og ajourholde tilgangene kan delegeres til en eller flere medarbeidere.

5.8 Internrevisjonen

For å styrke den interne kontrollen med sikkerhetsområdet er det viktig å ha en uavhengig

vurdering av området som helhet og av om de enkelte tiltakene følges. Dette må skje i tillegg til de kontrollene som gjøres for å ivareta regimeansvaret. Internrevisjonen velger sine revisjonsoppdrag på fritt grunnlag blant alle enheter i Arbeids- og velferdsetaten og utfører på denne måten uavhengige revisjoner av styringssystemet.

Planer for sikkerhetsgjennomganger som skal utføres av Sikkerhetsseksjonen, utveksles med Internrevisjonen for å oppnå synergieffekter og unngå unødig dobbeltarbeid. Internrevisjonen tar hensyn til og kan bygge sitt arbeid på det som gjøres av Sikkerhetsseksjonen.