Samarbeidsavtale om digitale tjenester for de kommunale sosiale tjenestene

Avtale mellom Eksempel kommune og
Arbeids- og velferdsdirektoratet

INNHOLDSFORTEGNELSE:

1 AVTALENS PARTER 3

2 BAKGRUNN 3

3 AVTALENS FORMÅL OG OMFANG 3

4 FORHOLDET TIL ANDRE AVTALER 3

5 SELVBETJENINGSLØSNINGEN «DITT NAV» PÅ NAV.NO 3

6 PARTENES FORPLIKTELSER 4

7 TAUSHETSPLIKT OG TILGANG TIL PERSONOPPLYSNINGER 5

8 SPERRING AV TILGANG TIL OPPLYSNINGER FOR ANDRE ENHETER I ARBEIDS- OG VELFERDSFORVALTNINGEN 5

9 AUTORISASJONS- OG TILGANGSKONTROLL 5

10 LAGRING 5

11 INNSYN, UTLEVERING OG RETTING ELLER SLETTING AV OPPLYSNINGER 5

12 BRUKERSTØTTE (IT-HJELPEN) 6

13 TILGANG TIL OPPLYSNINGER/STATISTIKK 6

14 VARSLING OG HÅNDTERING AV AVVIK 6

15 AVTALENS VARIGHET 6

16 SIGNERING AV AVTALEN OG IKRAFTTREDELSE 7

VEDLEGG 7

1 AVTALENS PARTER

Avtalens parter er Arbeids- og velferdsdirektoratet ved Arbeids- og velferdsetaten (org.nr. 889 640 782) og Eksempel kommune (org.nr. 123456789, kommune nr. 123). Disse omtales videre som parter.

2 BAKGRUNN

Arbeids- og velferdsdirektoratet har i samarbeid med kommunene og KS utviklet digitale tjenester for de kommunale sosiale tjenestene.

Det er utviklet en digital veiviser for økonomisk stønad etter sosialtjenesteloven (økonomisk sosialhjelp), og en digital søknad for økonomisk sosialhjelp.

Partene samarbeider om å utvikle nye digitale tjenester fortløpende for de kommunale sosiale tjenestene. Eksempel på nye digitale tjenester er innsyn og sikker elektronisk dialog mellom NAV-kontoret og innbyggeren.

3 AVTALENS FORMÅL OG OMFANG

Formålet med avtalen er å kunne tilby de som oppholder seg i den enkelte kommune tilgang til digitale tjenester for de kommunale sosiale tjenestene, og gi bedre service og tjenester til innbyggerne.

Denne avtalen regulerer samarbeidet mellom partene om bruk av de digitale tjenestene for de kommunale sosiale tjenestene.

Omfanget av de digitale tjenestene for de kommunale sosiale tjenestene vil fremgå av den til enhver tid gjeldende databehandleravtale mellom Arbeids- og velferdsdirektoratet og kommunen. Den enkelte tjeneste vil fremgå av databehandleravtalens vedlegg om databehandlingens omfang for den enkelte tjeneste.

Nye digitale tjenester for de kommunale sosiale tjenestene som utvikles vil derfor kreve at partene godkjenner supplerende vedlegg til inngått databehandleravtale før tjenesten kan tas i bruk.

4 FORHOLDET TIL ANDRE AVTALER.

Denne avtalen må ses i sammenheng med databehandleravtalen inngått mellom Arbeids- og velferdsdirektoratet og kommunen, og andre avtaler inngått mellom Arbeids- og velferdsetaten og den enkelte kommune.

Denne avtalen og databehandleravtalen mellom partene skal sikre personvernet i de digitale tjenestene for de kommunale sosiale tjenestene som Arbeids- og velferdsdirektoratet tilbyr alle landets kommuner.

5 SELVBETJENINGSLØSNINGEN «DITT NAV» PÅ NAV.NO

De digitale tjenestene for de kommunale sosiale tjenestene skal gi brukerne like muligheter til å søke elektronisk som søkere av statlige tjenester, og gis mulighet til å henvende seg digitalt til NAV-

kontoret. Selvbetjeningsløsninger vil gjøre det mulig for NAV-kontoret å frigjøre tid ved å forenkle saksbehandlingsprosessen, til å følge opp de brukerne som har størst bistandsbehov.

Brukere som ikke kan nyttiggjøre seg av digitale løsninger, skal fortsatt ha et tilbud via telefon til kontaktsenteret, henvendelse per post eller ved personlig oppmøte på NAV-kontoret.

De digitale tjenestene for de kommunale sosiale tjenestene vil være tilgjengelig for innbyggerne på selvbetjeningsløsningen «Ditt NAV» via nav.no og for kommunene i deres fagsystemer ved NAV-kontorene.

Selvbetjeningsløsningen forutsetter at bruker logger inn på nivå 4 med BankID eller tilsvarende.

Arbeids- og velferdsdirektoratet forvalter og driver selvbetjeningsløsningen «Ditt NAV» på nav.no som brukes til å tilby de digitale tjenestene for de kommunale sosiale tjenestene.

6 PARTENES FORPLIKTELSER

Partene forplikter seg til å samarbeide om å tilby best mulig digitale tjenester for brukere av de kommunale sosiale tjenestene og de ansatte på NAV-kontoret.

Kommunen er behandlingsansvarlig for personopplysningene i de digitale kommunale sosiale tjenestene og skal sikre at behandling av personopplysningene skjer i samsvar med personvernregelverkets bestemmelser.

Arbeids- og velferdsdirektoratet er databehandler på vegne av kommunen og ansvarlig for å sikre at opplysningene som registreres i selvbetjeningsløsningen på nav.no behandles i samsvar med personvernregelverkets bestemmelser og behandlingsansvarliges instrukser.

Arbeids- og velferdsdirektoratet opptrer på instruks fra kommunen som behandlingsansvarlig fra nav.no frem til KS sin tjeneste FIKS.

Partene skal sammen sørge for at de opplysninger som blir behandlet i selvbetjeningsløsningen på nav.no, ikke benyttes til andre formål enn det de er innhentet for, og at opplysningene kun er tilgjengelig for de medarbeidere som har tjenstlig behov for opplysningene. Arbeids- og velferdsdirektoratet plikter ellers å bistå kommunen i oppgaver etter personvernregelverket.

Partene er sammen ansvarlig for opplæring av de ansatte i selvbetjeningsløsningen for de digitale kommunale sosiale tjenestene på nav.no.

Partene skal følge felles sikkerhetsnormer for Arbeids- og velferdsforvaltningen, se databehandleravtalens vedlegg om tekniske og organisatoriske sikkerhetstiltak.

Dersom Arbeids- og velferdsdirektoratet vurderer endringer i rutiner og normer når det gjelder kommunens bruk av selvbetjeningsløsningen for de digitale kommunale sosiale tjenestene på nav.no skal kommunen orienteres.

7 TAUSHETSPLIKT OG TILGANG TIL PERSONOPPLYSNINGER

Tilgangen til personopplysninger i de digitale tjenestene for de kommunale sosiale tjenestene reguleres av taushetspliktbestemmelsene i NAV-loven §§ 7, lov om sosiale tjenester i arbeids- og velferdsforvaltningen § 44, jf. forvaltningsloven §§ 13 til 13 e.

Alle medarbeidere er underlagt taushetsplikt og plikter dermed å hindre at andre får adgang eller kjennskap til taushetsbelagt informasjon. Dersom informasjonen likevel skal deles, må det foreligge rettslig grunnlag for dette, f. eks gjennom samtykke eller lovhjemmel.

Partene skal i tillegg bevare taushet om alle konfidensielle opplysninger og materiale, herunder kunnskap om sikkerhetsrutiner mv. som partene får kjennskap til i forbindelse med inngåelse og oppfyllelse av denne avtalen.

Opplysninger skal ikke behandles og være tilgjengelig for andre formål enn det de er samlet inn for eller eventuelt andre formål som er forenlig med dette. "Need to know"-prinsippet innebærer at den behandlingsansvarlige og databehandleren skal sørge for rutiner som sikrer at medarbeidere kun har tilgang til de opplysninger som han eller hun trenger for å utføre sine arbeidsoppgaver.

8 SPERRING AV TILGANG TIL OPPLYSNINGER FOR ANDRE ENHETER I ARBEIDS- OG VELFERDSFORVALTNINGEN

Personopplysninger i de digitale tjenestene for de kommunale sosiale tjenestene er ikke gjenstand for behandling av Arbeids- og velferdsdirektoratet og vil bli sperret for tilgang fra andre enheter i Arbeids- og velferdsforvaltningen. Teknisk personell i Arbeids- og velferdsdirektoratet som drifter løsningen vil ha tilgang til løsningen for å sikre at den fungerer etter hensikten.

9 AUTORISASJONS- OG TILGANGSKONTROLL

Teknisk personell tilknyttet drift og brukerstøtte i Arbeids- og velferdsdirektoratet som har oppgaver knyttet til søknadsløsningen er underlagt taushetsplikten i NAV.

10 LAGRING

Personopplysninger skal ikke lagres lenger enn nødvendig. Søknader som ikke blir sendt fra bruker vil bli midlertidig lagret i en periode på inntil tre måneder. Mellomlagring vil gi brukeren mulighet til å fortsette å fylle ut søknaden uten å måtte starte prosessen pånytt. Når bruker trykker send, blir søknaden sendt videre til kommunen via FIKS meldingsutveksler. Kopi av søknad registreres i "juridisk logg" når bruker trykker send for å sikre bevis på hvordan meldingen ser ut når den ble sendt fra bruker. Juridisk logg vil være tilgjengelig ved en eventuell rettslig tvist.

Løsningen er utarbeidet slik at personopplysninger ikke lagres lengre enn det som er nødvendig for formålet med selvbetjeningsløsningen på nav.no, samt å sikre kommunens kassasjonsregler etter arkivloven.

11 INNSYN, UTLEVERING OG RETTING ELLER SLETTING AV OPPLYSNINGER

Hver av partene er ansvarlige for å gi innsyn, utlevere, rette eller slette opplysninger i hht.de respektive regelverk. Se også databehandleravtalens punkt 5 om dette.

12 BRUKERSTØTTE (IT-HJELPEN)

Kommunen kan vederlagsfritt benytte Arbeids- og velferdsdirektoratet sin brukerstøtte for selvbetjeningsløsningen «Ditt NAV». Alle henvendelser om feil skal meldes til Team selvbetjening på e-post nav.it.team.selvbetjening@nav.no.

13 TILGANG TIL OPPLYSNINGER/STATISTIKK

Det vil ikke bli hentet ut statistikk om brukere med oversikt over personopplysninger fra selvbetjeningsløsningen. Kun statistikk i form av antall søknader som sendes, tidspunkt for når løsningen brukes, hvilke medier som brukes (telefon, nettbrett og lignende) og lignende vil bli utarbeidet med sikte på å videreutvikle tjenestene. Slik statistikk vil være anonymisert og ikke inneholde personopplysninger om personer som bruker løsningen.

14 VARSLING OG HÅNDTERING AV AVVIK

Partene har gjensidig varslingsplikt hvis det oppdages, eller man har mistanke om, brudd på avtalens bestemmelser.

Varslingen skal skje via oppnevnte kontaktpersoner som fremgår av databehandleravtalen.

15 AVTALENS VARIGHET

Denne avtalen gjelder så lenge det foreligger en databehandleravtale mellom partene. Oppsigelse av denne avtalen eller databehandleravtalen vil innebære oppsigelse av begge avtalene.

16 SIGNERING AV AVTALEN OG IKRAFTTREDELSE

Avtalen trer i kraft fra det tidspunkt begge partene har signert samarbeidsavtalen og databehandleravtalen elektronisk. Det samme gjelder for avtalenes vedlegg. Nye vedlegg til avtalen må også signeres elektronisk av begge parter før de er gyldige.

VEDLEGG

1. Felles sikkerhetsnormer for Arbeids- og velferdsforvaltningen

VEDLEGG

Felles sikkerhetsnormer

For Arbeids- og velferdsforvaltningen

Dette dokumentet omfatter felles sikkerhetsnormer for Arbeids- og velferdsforvaltningen som skal sikre felles forståelse mellom stat og kommune i forhold til sikkerhetsnivå ved etablering av felles lokalt kontor. Dokumentet inneholder konkretisering av lovmessige krav som alle enheter i Arbeids- og velferdsforvaltningen bør implementere. Det presiseres at med Arbeids- og velferdsforvaltningen (også omtalt som forvaltningen) menes her summen av 1) statlige enheter og 2) enheter hvor stat og kommune er samlokalisert.

For spørsmål knyttet til dette dokumentet – kontakt din nærmeste sikkerhetskoordinator.

17 ENDRINGSLOGG

Vs.	Dato	Kapittel	Endring	Produsent/eier	Godkjent av
1.0	22.08.06	Alle	Fremleggelse i direktørmøtet	Sikkerhetsledelsen	Tor Saglie
1.2	24.11.06	1 1.4 og Appendiks B 1.3. Fjernet appendiks C, D og E	Oppdatering etter innspill fra KS	PIB NDU	Morten Nilsen Skogvik
1.3	11.04.07	Appendiks A og B	Oppdateringer	PIB NDU	Sikkerhetsrådet

INNHOLDSFORTEGNELSE

1. FELLES SIKKERHETSNORMER 3

1.1 BAKGRUNN OG HENSIKT 3
1.2 MÅLGRUPPE 3
1.3 ANSVAR 3
1.4 OPPLÆRING OG KOMPETANSE 4
1.5 LOKAL VS. SENTRAL STYRING AV SIKKERHET 4
1.6 RAPPORTERING 4
1.7 SIKKERHETSINSTRUKSER 5

2. VEDLEGG 5

2.1 VEDLEGG A: MAL – «LOKAL SIKKERHETSINSTRUKS FOR ENHETENE» 5
2.2 VEDLEGG B: MAL – «LOKAL BEREDSKAPSPLAN FOR ENHETENE» 5

APPENDIKS A: SIKKERHETSINSTRUKS FOR MEDARBEIDER 6

APPENDIKS B: TILLEGGSINSTRUKS FOR LEDER 12

1. FELLES SIKKERHETSNORMER

1.1 BAKGRUNN OG HENSIKT

Arbeids- og velferdsforvaltningen behandler store mengder informasjon med beskyttelsesbehov, både manuelt og elektronisk. Både stat og kommune er avhengig av at brukere, oppdragsgivere, samarbeidspartnere og tilsynsmyndigheter har tillit til at forvaltningen av informasjonen skjer på en sikker og kvalitetsmessig forsvarlig måte.

Partene (stat og kommune) er behandlingsansvarlige etter personopplysningsloven for egne ansvarsområder, og har således hver for seg plikt til å oppfylle lovens krav. I tillegg kommer utfordringen spesielt knyttet til ivaretakelse av personvern ved etablering av nye felles lokale kontor som skal sikre et mer koordinert og samordnet tjenestetilbud for flerbrukere.

Uklarheter og lokale variasjoner kan føre til et vanskeligere forhold til tilsynsmyndigheter, større mengde oppfølgingsarbeid, mindre etterprøvbar sikkerhet og fare for et "ujevnt" nivå på personvernet i den nye forvaltningen. Det vil videre være uheldig dersom medarbeiderne må forholde seg til en rekke nesten tilsvarende krav og til enhver tid holde rede på hvilke krav som gjelder for hvilken behandling.

Den totale sikkerheten i Arbeids- og velferdsforvaltningen er avhengig av tilfredsstillende sikkerhet i både statlig og kommunal del. Sikkerheten må derfor reguleres helhetlig, slik at begge parter kan oppfylle de lovmessige krav som regulerer begges virksomhet. Partene bør derfor enes om å legge disse felles normene til grunn.

Det er verdt å merke seg at begrepet *sikkerhet* her defineres videre enn det normalt sett tolkes, da det favner om både personvern-, informasjonssikkerhets- og beredskapsområdet.

1.2 MÅLGRUPPE

Dette dokumentet er utformet for alle enheter i Arbeids- og velferdsforvaltningen, uavhengig av om dette er statlige enheter, eller samlokaliserte enheter bestående av stat og kommune.

Målgruppen for dette dokumentet med tilhørende vedlegg er først og fremst alle enhetsledere i forvaltningen. Dokumentet inneholder også informasjon og instrukser som er gjeldende for alle medarbeidere i Arbeids- og velferdsforvaltningen.

1.3 ANSVAR

Sikkerhet er et linjeansvar. Enhetsleder har ansvaret for å etablere og opprettholde et tilstrekkelig sikkerhetsnivå innen sin enhet, herunder ansvaret for;

- ✓ At innholdet i dette dokumentet gjøres tilstrekkelig kjent i egen enhet, og at alle medarbeidere har tilstrekkelig kunnskap, ferdigheter og holdninger om personvern, informasjonssikkerhet og beredskap

- ✓ At medarbeidere, innleide konsulenter og eventuelt fagansvarlige og prosjektledere, er orientert om, og settes inn i den enkelte kommunes og Arbeids- og velferdsetatens grunnleggende sikkerhetskrav og sikkerhetsrutiner
- ✓ At sikkerhetshendelser i egen enhet rapporteres og håndteres, og at nødvendige tiltak treffes for å begrense skader og konsekvenser

1.4 OPPLÆRING OG KOMPETANSE

Tilfredsstillende sikkerhet er et resultat av både tekniske, organisatoriske og miljømessige tiltak. Undersøkelser viser at hovedtyngden av sikkerhetshendelser er relatert til menneskelige feil, noe som betyr at det å skape en robust og felles *sikkerhetskultur* er viktig.

Enhetsleder er ansvarlig for at alle medarbeidere (både faste og midlertidige) får opplæring innen sikkerhetsområdet. Dette omfatter bl.a. at alle medarbeidere skal gjøres kjent med, sette seg inn i, samt undertegne Appendiks A – «Sikkerhetsinstruks for medarbeidere». Alle enheter har også tilgang til en sikkerhetskoordinator. Denne sikkerhetskoordinatoren skal bistå enhetsleder bl.a. i arbeidet med opplæring og kompetanseutvikling av den enkelte enhets medarbeidere. I felles lokalt kontor vil dette ansvaret være pålagt både en kommunal og en statlig sikkerhetskoordinator.

1.5 LOKAL VS. SENTRAL STYRING AV SIKKERHET

For kommunens del, er behandlingsansvaret etter personopplysningsloven et ansvar som ligger i kommunen. For Arbeids- og velferdsetatens del, er det derimot Arbeids- og velferdsdirektøren som er behandlingsansvarlig. Selv om det daglige ansvaret er delegert til lokal enhetsleder er statsetaten avhengig av sentral styring av sikkerheten for å sikre reell kontroll av de plikter som tilligger Arbeids- og velferdsdirektøren som behandlingsansvarlig. Videre er det nødvendig å sikre at behandlingene, og dermed sikkerhetsnivået for den enkelte bruker, er tilstrekkelig likt uavhengig av hvor vedkommende bor eller henvender seg i landet.

Det er likevel visse forhold det ikke vil være mulig å gi eksakte sentrale føringer for, da ivaretakelsen er helt avhengig av lokale forhold. Dette gjelder bl.a. fysisk sikkerhet som skal iverksettes og dokumenteres lokalt på bakgrunn av de sentrale føringer som det er mulig å gi. Valg av sikringstiltak skal da baseres på risikovurdering og vurdering ut fra prinsippet om et rimelig forhold mellom tilgjengelige ressurser, og hvilken grad av sikkerhet det er mulig å oppnå. Fysiske sikringstiltak skal også omfatte beskyttelse av taushetsplikt og personvernhensyn i forvaltningens møte med brukere.

De sentrale sikkerhetskrav kan ikke fravikes, med mindre det handler om å styrke kravene for å ivareta den enkelte kommunes behov.

1.6 RAPPORTERING

Det er viktig at sikkerhetshendelser rapporteres, uansett hvor små og ubetydelige de kan se ut å være. Arbeids- og velferdsforvaltningen har behov for å kunne vurdere om sikkerhetstiltakene i sum fungerer tilstrekkelig.

Enhetsleder skal varsles om sikkerhetsmessige hendelser i egen enhet. Enhetsleder skal se til at nødvendige tiltak treffes for å begrense skader og konsekvenser. Enkelte sikkerhetshendelser skal uten opphold varsles direkte til Arbeids- og velferdsetaten, eller til den enkelte kommune. Eksempler på rapporteringsverdige sikkerhetshendelser er forsøk på inntrenging og misbruk av IKT-systemer, urettmessig endring, sletting, utlevering av informasjon, innbrudd i lokaler, uvedkommendes tilgang til systemer, utstyr og informasjon osv.

Arbeids- og velferdsetaten og den enkelte kommune har ulike rutiner for innrapportering av sikkerhetshendelser. Disse rutiner skal beskrives i vedlegg A – «Lokal sikkerhetsinstruks for enhetene». Det er viktig at rutinene utdypes slik at det ikke er unødig tvil om hva som skal reguleres hvor.

1.7 SIKKERHETSINSTRUKSER

Organisatoriske sikkerhetstiltak innebærer at arbeid og ansvar skal være organisert på en slik måte at tilfredstillende sikkerhet kan oppnås. Av den grunn må ansvars- og myndighetsforhold være tydelig og kjent for dem det gjelder. Ansvar, myndighet og oppgaver for medarbeidere er derfor nedfelt i egne instrukser. Se Appendiks A og B.

2. VEDLEGG

Målgruppen for vedleggene nedenfor (vedlegg A og B) er først og fremst enhetsledere og medarbeidere med oppgaver innen sikkerhetsområdet. Det er enhetsleders ansvar å vurdere om noe av innholdet i vedleggene må gjøres kjent for enhetens øvrige medarbeidere.

2.1 VEDLEGG A: MAL – «LOKAL SIKKERHETSINSTRUKS FOR ENHETENE»

Dette vedlegget skal brukes av enhetsleder for å dokumentere de *lokale valgene* som gjøres i den enkelte enhet. Risikovurdering skal gjennomføres og benyttes som et utgangspunkt for valg og prioritering av sikkerhetstiltak. Mal for gjennomføring av en enkel risikovurdering er et eget skjema i vedlegget.

Se vedlagte mal (lenke).

2.2 VEDLEGG B: MAL – «LOKAL BEREDSKAPSPLAN FOR ENHETENE»

Vedlegget skal brukes for å planlegge hvordan enhetsleder og enheten skal håndtere uforutsette krisesituasjoner, samt krise i fred og krig, for å motvirke de negative konsekvenser som eventuelt kan oppstå ved avbrytelser i daglig drift av informasjonssystemer og forvaltningstjenester.

Se vedlagte mal (lenke).

Felles sikkerhetsnormer for Arbeids- og velferdsforvaltningen
Sikkerhetsinstruks for medarbeider

18 APPENDIKS A: SIKKERHETSINSTRUKS FOR MEDARBEIDER

Denne sikkerhetsinstruksen gjelder for alle medarbeidere i Arbeids- og velferdsforvaltningen, uavhengig av om vedkommende er ansatt i stat eller kommune. Instruksen er en del av lokal samarbeidsavtale mellom statsetaten og den enkelte kommune. Eventuelle tileggskrav må dokumenteres lokalt.

Sikkerhetsinstruksen gjelder for alle typer oppgaver og funksjoner dersom det ikke foreligger annen avtale eller instruks. Sikkerhetsinstruksen skal undertegnes av den enkelte medarbeider. Enhver som utfører tjeneste eller arbeid for Arbeids- og velferdsforvaltningen har taushetsplikt, og skal i tillegg til denne sikkerhetsinstruksen undertegne taushetserklæring.

I denne instruksen brukes begrepet IKT Drift. Begrepet omfatter både den IKT funksjonen som Arbeids- og velferdsetaten har, og den IKT funksjonen som den enkelte kommune har. Lokal sikkerhetsinstruks bør regulere nærmere hva som skal håndteres hvor.

1. FYSISK ADGANGSKONTROLL

1.1 – Adgangskort og nøkler:

- Alle medarbeidere skal bære tydelig synlig adgangskort. Der dette ikke er hensiktsmessig, skal det på annen måte utøves tilfredstillende adgangskontroll.
- Dersom adgangskort/nøkler mistes/blir stjålet, skal dette straks meldes til enhetsleder. Adgangskortet vil da bli stengt slik at ingen kan misbruke det.
- Medarbeidere som slutter eller går ut i permisjon, skal levere adgangskort/nøkler tilbake til enhetsleder;
    - Unntak: medarbeidere i permisjon dersom jobbrelaterte hensyn tilsier dette, og forutsatt at dette er avtalt med, og dokumentert av, nærmeste enhetsleder.

1.2 – Besøkende:

- Den som mottar besøk, er ansvarlig for at besøkende kun oppholder seg i områder som besøkende skal ha adgang til. Besøkende skal ikke oppholde seg i avlåste eller avsperrede deler av forvaltningens lokaler uten følge av en autorisert medarbeider;
    - Den besøkende kan i særlige tilfeller oppholde seg i lokalet uten følge, forutsatt at medarbeideren er til stede, og at dette er eksplisitt godkjent av enhetsleder.
- Personer som oppholder seg utenfor tillatte områder i forvaltningens lokaler, uten følge av en autorisert medarbeider eller uten adgangskort, skal bortvises eller henvises til leder av den som påtreffer en slik person.

2. BRUK AV FORVALTNINGENS IKT-SYSTEMER

2.1 – Godkjent bruk:

- Forvaltningens IKT-systemer skal benyttes til de formål som de er godkjent for. Det oppfordres til å ikke bruke datasystemene til personlige formål, herunder privat e-post og private filer;
    - Begrenset bruk kan tolereres dersom lagret i katalog på personlig område, og tydelig merket med «Privat». Dette må imidlertid ikke påvirke jobbrelaterte oppgaver eller være i strid med denne instruks, lover eller allmenne normer for oppførsel eller sosial adferd, og må holdes på et minimumsnivå. Det vil si at det ikke aksepteres lagring av private bilder, video, musikkfiler ol.

- Jobbrelaterte filer og informasjon skal lagres på serverne. Dette skal ikke lagres på lokal harddisk. Det henspeiles her på saksbehandlerinformasjon.
- Medarbeidere har et medansvar for å ta initiativ til justering av tilganger i IKT-systemene, slik at privilegier i IKT-systemene gjenspeiler medarbeiderens tjenestelige behov.
- Tilgang til IKT-systemene skal ikke misbrukes til å på eget initiativ foreta kartlegging eller testing av mulige systemsvakheter, forsøke å omgå forvaltningens sikkerhetsmekanismer, tilegne seg utvidede tilgangsrettigheter på lokal maskin eller utnytte eventuelle sikkerhetssvakheter.

2.2 – Logging:

- Internettrafikk, nettverkstrafikk og bruk av systemer i forvaltningens nettverk, blir logget for administrasjon og sikkerhet. Dette betyr at medarbeideres aktiviteter blir registrert, og at det er mulig å spore tilbake om det oppdages brudd på interne retningslinjer.
- Autorisert personell gjennomgår loggene rutinemessig og iverksetter tiltak om nødvendig.

2.3 – Eierskap, ansvar og innsynsrett:

- IKT-utstyr, programvare og lagret informasjon, er forvaltningens eiendom og ansvar.
- Forvaltningen forbeholder seg rett til innsyn i all informasjon lagret i IKT-systemene begrunnet ut fra virksomhetens behov. Ved uforutsett fravær kan leder søke NDU PIB om innsyn i e-postkassen, personlig hjemmekatalog ol for tilgang til tjenesterelaterte dokumenter. Innsyn gjennomføres av NDU PIB etter fastsatt prosedyre, m/ tillitsvalgt eller objektiv part tilstede. Hvis mulig vil man før innsynretten praktiseres, innhente samtykke fra den medarbeideren det gjelder. Dersom dette ikke lar seg gjøre vil tillitsvalgt eller annen objektiv part ivareta medarbeiderens interesser.

2.4 – Godkjent IKT-utstyr:

- Det skal kun benyttes IKT-utstyr, lagringsmedia og programvare på forvaltningens nettverk som er anskaffet og godkjent av IKT Drift;
  - All installasjon av utstyr og programvare skal gjøres av medarbeidere som har godkjennelse til å gjøre dette, eller av andre som er utpekt til å gjøre denne jobben.
  - Behov for programvare utenom det som forvaltningen tilbyr som standard programvare må godkjennes av enhetsleder og IKT Drift.
- Dataskjermer skal plasseres slik at det ikke er innsyn for uvedkommende.
- Det skal ikke tilkobles privat utstyr i nettverket. Dette gjelder også privat PDA og mobiltelefon.
- Konsulenter og vikarer skal ikke benytte egen PC i nettverket, men få tildelt maskin av forvaltningen;
  - Særskilte behov for bruk av egen PC skal avklares med enhetsleder.
- Kun godkjente separate eksterne forbindelser kan kobles til forvaltningens nettverk.
- Hjemmekontor og hjemmekontorutstyr skal benyttes slik at ikke-ansatte ikke får tilgang til jobbrelatert informasjon og data.
- Medarbeidere som slutter eller går ut i langvarig permisjon, skal levere alt utlevert IKT-utstyr og programvarelisenser til sin enhetsleder;
  - Unntak fra denne regel er mulig for medarbeidere i permisjon dersom jobbrelaterte hensyn tilsier dette og forutsatt at dette er avtalt med nærmeste leder.

2.5 – Bærbart IKT-utstyr:

Med bærbart IKT-utstyr menes bærbar PC, PDA, mobiltelefon, kamera, lagringsmedia ol.;

- Utstyret er medarbeiderens ansvar og det skal beskyttes mot hærverk, tyveri og misbruk. Det er ikke tillatt å forlate utstyret uten tilfredstillende sikring. Et eksempel på tilfredstillende sikring er bruk av sikkerhetswire. Sikkerhetswire fås ved å kontakte IKT Drift.
- Utstyret skal ikke benyttes av andre enn medarbeideren selv.
- Ved reise skal utstyr alltid være under oppsyn og alltid medbringes som håndbagasje på fly.
- Tilgang til utlevert utstyr er tidsubestemt. Enhetsleder kan til enhver tid kreve tilbakelevering.
- Medarbeideren har vanlig aktsomhetsansvar ved skade/tap på utstyret.
- Når bærbar PC ikke er koblet opp mot forvaltningens nettverk, kan direkte tilkobling til Internett etableres. Medarbeideren rådes til alltid å koble seg til Internett via forvaltningens nettverk, for å ha tilfredsstillende beskyttelse mot kode med ondsinnet innhold.
- Det skal ikke overføres, klippes fra, eller synkroniseres mot andre dokumenter, tjenester eller informasjon til PDA/mobiltelefon fra forvaltningens nettverk.
- Når lagringsmedier benyttes på bærbart utstyr, skal disse viruskontrolleres.

2.6 – Identitetskontroll: pålogging og avlogging, brukernavn og passord, skjermsparer:

- Hver bruker har en egen brukerident med tilhørende passord. Passordet, og eventuelt passordgenerator for fjerntilgang/hjemmekontor, skal ikke oppgis til eller lånes til andre.
- Det er ikke tillatt å bruke en annens brukerident.
- Passord skal ikke skrives ned.
- Passord skal endres regelmessig, systemet varsler automatisk når dette skal gjøres.
- Ved mistanke om at passordet ditt er blitt kjent av andre, skal passordet endres umiddelbart.
- Passordbeskyttet skjermsparer skal benyttes når arbeidsstasjonen forlates.
- Medarbeidere skal alltid logge seg ut før maskinen overlates til andre og ved arbeidstidens slutt.

3. INFORMASJONSHÅNDTERING

Personopplysningsloven gjelder helt fra det er registrert enkle opplysninger vedrørende en enkeltperson;

- Personopplysninger i forvaltningen skal ikke gjøres tilgjengelig for uautoriserte medarbeidere eller uvedkommende.
- Det skal ikke søkes etter opplysninger om personer som du ikke har bruk for i det daglige arbeid. Alle autoriserte oppslag skal ta utgangspunkt i om det foreligger et tjenestlig behov.
- Håndtering av trusselutsattes personopplysninger følger særlige rutiner, se disse.
- Beskyttelsesverdig informasjon, f.eks. avtaler, bedriftshemmeligheter, skal ikke gjøres tilgjengelig for uautoriserte medarbeidere eller uvedkommende.
- Den som produserer et dokument skal vurdere om innholdet er av sensitiv karakter. Sensitive dokumenter skal beskyttes, merkes og behandles i henhold til gradering.
- Den som produserer eller behandler et gradert dokument skal behandle det i henhold til sikkerhetslovens krav.
- Lagringsmedia som inneholder sensitive personopplysninger, bedriftshemmeligheter eller gradert materiale skal merkes iht. sentrale retningslinjer.
- Utskrifter skal hentes umiddelbart, der funksjon for konfidensiell utskrift er tilgjengelig skal denne benyttes ved utskrift av beskyttelsesverdig informasjon.

3.1 – Lagring:

- Sensitive personopplysninger er kun tillatt å lagre i godkjente fagapplikasjoner på forvaltningens nettverk;
  - Bruk av ikke-fagapplikasjoner, som f.eks Word, Excel, for skriving av notater, rapporter og tilsvarende, for lagring av personopplysninger, er kun tillatt dersom dette er tiltenkt som midlertidig lagring. Denne midlertidige lagringen skal bare skje på enhetens fellesområde/hjemmeområde på serveren. Notatene skal slettes etter de er godkjent, eventuelt lagt inn i fagapplikasjoner og skrevet ut. Der det brukes wordfiler etc som flerbrukersystem, i mangel av tilfredsstillende fagsystem, skal dette dokumenteres jfr vedlegg lokal sikkerhetsinstruks – skjema B, samt lagres på tilgangsstyrt område.
  - Personopplysninger skal bare lagres lokalt på PC eller på portabelt utstyr som bærbar PC, minnepinner ol. dersom det er innhentet godkjenning fra leder og forutsatt at lagring skjer med løsninger godkjent av IKT Drift.
  - Sensitive personopplysninger kan kun lagres på portabelt utstyr dersom det lagres kryptert.
- Når lagringsmedia eller dokumenter med sensitive personopplysninger ikke er under direkte oppsyn, skal de nedlåses i skap/skuff, eller kontor avlåses, slik at uvedkommende ikke får tilgang.

3.2 – Dokumentforsendelse:

- Dokumenter og lagringsmedia med taushetsbelagt og beskyttelseverdig informasjon skal alltid forsendes i gjenlimt konvolutt/forseglet innpakning.
- Avsender er alltid ansvarlig for å forsikre seg om at mottaker er autorisert for å kunne motta og behandle opplysningene.
- Telefaks skal ikke benyttes til å sende dokumenter inneholdende taushetsbelagt eller beskyttelsesverdig informasjon.

3.3 – Elektronisk kommunikasjon (bl.a. e-post):

- Privat e-post skal lagres i en egen mappe merket «Privat».
- Personopplysninger skal ikke sendes via telefaks.
- Personopplysninger skal bare sendes elektronisk, f.eks. via e-post, dersom det benyttes kryptert sikkerhetsløsning godkjent av IKT Drift. Slik løsning foreligger på NAVs interne nettverk, - **fra** @nav.no **til** @nav.no adresse.
- Sensitiv informasjon skal ikke sendes elektronisk uten godkjent krypteringsløsning. Prosedyre vil bli utviklet.
- Avsender er alltid ansvarlig for å forsikre seg om at mottaker er autorisert for å motta og behandle opplysningene.
- Det må vurderes om kopi av e-post skal journalføres.
- Massedistribusjon av informasjon skal være jobbrelatert;
  - E-postmeldinger skal kun sendes til mottakere som trenger informasjonen.
- Medarbeidere skal være skeptisk til filvedlegg fra ukjent avsender, og til filvedlegg fra kjent avsender som har merkelig navn, tittel eller på annen måte skiller seg fra e-post som pleier på komme fra avsender. Vedlegg kan inneholde virus.
- Mottakere som får feilsendt e-post skal slette disse umiddelbart.

3.4 – Innsyn, utlevering og retting/sletting av informasjon:

- Den registrerte har rett til innsyn i opplysninger om seg selv enten disse er registrert i den enkelte fagapplikasjon eller fremkommer av papirbaserte saksmapper. Alle medarbeidere skal derfor kjenne til rutinebeskrivelser for innsynshåndtering, og være i stand til å finne frem til spesialrapporter til dette formål, utskrifter av øvrig lagret informasjon og riktig håndtering av innsyn i forhold til de aktuelle saksmapper.
- I all hovedsak skal begjæringer om retting/supplering av mangelfulle personopplysninger foretas ved at feil eller mangelfulle opplysninger markeres, og at nye opplysninger påføres eller suppleres. Det hører til unntakstilfellet at opplysninger blir slettet. Alle medarbeidere skal derfor kjenne til hva som er riktig håndtering av og kriterier for innvilgelse av ønsker om rettelse og sletting av personinformasjon, se egen rutinebeskrivelse.
- Det skal aldri utleveres opplysninger uten at det foreligger et gyldig hjemmelsgrunnlag for utleveringen. Typiske grunnlag er uttrykkelig hjemmel i lov eller samtykke fra den det gjelder. I tillegg skal saksbehandler forvisse seg om at det er rette vedkommende utlevering skjer til.

3.5 – Makulering av dokumenter/kassering av utstyr:

- Dokumenter med taushetsbelagt og beskyttelseverdig informasjon makuleres gjennom bruk av makuleringsenhet godkjent for dette.
- Medarbeidere som slutter, skal rydde i egne filområder og e-post, og sikre at all relevant informasjon blir lagret på godkjent sted.
- Når ansettelsesforholdet avsluttes vil gjenværende informasjon på medarbeiderens områder bli slettet.
- Utstyr som inneholder lagringsmedier skal destrueres i henhold til godkjent prosedyre.

3.6 – Sikkerhetskopiering:

- For å sikre at det blir tatt sikkerhetskopier, skal jobbrelatert informasjon lagres på, eller eventuelt systematisk kopieres til, servere i nettverket. IKT Drift foretar regelmessig sikkerhetskopiering av all informasjon.
- Lokal harddisk på PC i nettverk blir det ikke tatt sikkerhetskopi av.

3.7 – Internett:

- Internett skal benyttes med sunn fornuft og varsomhet, og i samsvar med vanlige etiske normer;
  - Det er ikke tillatt å surfe på sider eller laste ned og/eller lagre filer som inneholder pornografi, opphavrettslig beskyttet materiale, som f.eks. musikk, filmer, programvare, eller informasjon som er støtende, trakasserende, obskøn, truende eller rasistisk. Slike filer blir i så fall slettet.
  - Det er ikke tillatt å laste ned og/eller installere programvare på forvaltningens IKT-utstyr. Se også punkt 2.4.
- Det er ikke tillatt å benytte fildelingstjenester.
- Ressurskrevende tjenester/applikasjoner, som ikke er jobbrelaterte, som f.eks. radiolytting og TV/video streaming tillates ikke.

3.8 – Reparasjon, service, vedlikehold og brukerstøtte:

- Ta kontakt med IKT Drift dersom du har mistanke om feil eller problemer med tilgang til systemer, tjenester eller informasjon.

3.9 – Avslutning av ansettelsesforhold:

- Ved avslutning av ansettelsesforhold skal medarbeidere uoppfordret levere IKT-utstyr og rydde, slette og/eller makulere informasjon og lagringsmedia i henhold til punktene over.

4. PERSONELL OG SIKKERHET

4.1 – Sikkerhetsbrudd:

- Uønskede hendelser og observerte sikkerhetsbrudd skal rapporteres til nærmeste enhetsleder. Hendelser knyttet til brudd på denne sikkerhetsinstruks, vurderes som et sikkerhetsbrudd.
- Brudd på sikkerhetsinstruksen vil bli behandlet som personalsak iht gjeldende rutiner for Arbeids- og velferdsetaten og/eller den enkelte kommune. Alvorlige brudd på reglene i denne sikkerhetsinstruksen vil kunne få konsekvenser for medarbeiderens arbeidsforhold, samt eventuelt resultere i strafferettslige reaksjoner.

4.2 – Kontakt med presse/media:

- Det er kun informasjonsansvarlig, eller bemyndigede personer, som har myndighet til å uttale seg til presse/media i forbindelse med saker som vedrører sikkerhet.

5. SIGNATUR

Denne side signeres, skrives ut og oppbevares i personalmappe til medarbeider eller avrop for konsulent.

Jeg bekrefter herved at sikkerhetsinstruks for medarbeider er lest og forstått:

Sted: _____ **Dato:** _____

Navn med blokkbokstaver: _____ **Signatur:** _____

_____

Felles sikkerhetsnormer for Arbeids- og velferdsforvaltningen
Tilleggsinstruks for leder

APPENDIKS B: TILLEGGSINSTRUKS FOR LEDER

Målgruppen er enhetsledere i Arbeids- og velferdsforvaltningen med personalansvar. Denne instruksen kommer i tillegg til Appendiks A.

1. ANSETTELSE ELLER INNLEIE AV PERSONELL

1.1 – Fysisk adgang:

- Leder skal sørge for at den enkelte medarbeider har fått utlevert adgangskort, nøkler ol., og at dette er registrert.
- Leder skal vurdere om enheten er så kompleks at besøkende skal registreres. Leder må fastsette regler og treffe tiltak om fysisk adgangskontroll for enheten, slik at det fremgår hva som er åpen sone (hvor publikum kan ferdes fritt), interne soner (hvor alle medarbeidere har adgang) og sikrede soner (hvor bare de som trenger det har adgang). Det må vurderes om det er hensiktsmessig at besøk registreres med dato, klokkeslett ol.

1.2 – Ansatte eller andre som kan få tilgang til personinformasjon:

- Leder skal sørge for at taushetspliktskjema for NAV er lest, og underskrevet av den enkelte medarbeider/innleide, før det gis tilgang til forvaltningens informasjon.
- Leder skal sørge for at alle medarbeidere/innleide er kjent med, har satt seg inn i og underskrevet sikkerhetsinstruksen for medarbeidere, jfr. Appendiks A.
- Leder skal sørge for at medarbeiderne har utstyr og mulighet for å overholde kravene i sikkerhetsinstruks for medarbeider.
- Leder skal ved organiseringen av arbeidet og tildeling av oppgaver sørge for at det tas tilstrekkelig hensyn til personvern og taushetsplikt.

1.3 – Tilgang til IKT-systemer og nettverk:

- Leder er ansvarlig for at ingen medarbeidere gis tilgang til IKT-systemer eller informasjon ut over det som helt nødvendig for å utføre pålagte arbeidsoppgaver (tjenestlig behov).
- Leder skal sørge for løpende vedlikehold av tildelte rettigheter i IKT-systemene.
- Leder er ansvarlig for at det gis tilstrekkelig opplæring til medarbeidere som har tilgang til IKT-systemene.
- Leder, eller den leder bemyndiger skal benytte IKT Drift (bl.a. «brukerhjelpa» og gjeldende regler/rutiner i kommunen) for bestilling av PC, tilgang til IKT-systemer, osv.

1.4 – Konsulenter og annet innleid personell:

- Sjekklisten over gjelder. I forbindelse med taushetserklæring kan alternativt virksomheten som står for utleie underskrive konfidensialitetserklæring forutsatt at alle deres ansatte allerede har underskrevet en intern taushetserklæring som er dekkende.

2. OPPLÆRING OG KOMPETANSEUTVIKLING

- Leder skal bygge grunnlag for motivasjon og engasjement blant sine medarbeidere og stimulere til god sikkerhetskultur i enheten.
- Leder er ansvarlig for at alle medarbeidere har fått nødvendig tilgang til, og forståelse av, forvaltningens krav til personvern, informasjonssikkerhet og beredskap.
- Leder er ansvarlig for at det legges til rette for, og gjennomføres, opplæringstiltak.
- Leder skal sørge for at enheten har kontakt med sikkerhetskoordinator til støtte i dette arbeidet.

3. INSTALLASJON AV PC OG PROGRAMVARE

- Leder skal kontakte IKT Drift ved behov for PC tilkoblet forvaltningens nettverk.
- Leder skal ved anskaffelse av IKT-utstyr sørge for at utstyret er innkjøpt, konfigurert og vedlikeholdt av IKT Drift.

4. REGELMESSIG VERIFIKASJON AV AUTORISERTE BRUKERE OG BRUKERTILGANGER

5. Leder skal regelmessig gjennomgå oversikten over brukere og brukertilganger. Leder skal så snart som praktisk mulig etter mottak;
   - Verifisere at oversikten er korrekt, dvs. reflekterer ansvars og organisatorisk tilhørighet for egne ansatte.
   - Bekrefte at oversikten er riktig, eller korrigere eventuelle feil og mangler.

196. REGELMESSIGE STIKKPRØVER PÅ SKRIVERE

- Leder, eller den leder delegerer dette til, skal regelmessig sjekke om det ligger igjen utskrifter på skrivere med beskyttelsesverdig innhold, samt sørge for at enheten har tilstrekkelig makuleringsrutiner og at disse benyttes.

6. ENDRING AV ARBEIDSFORHOLD/ANSVAR

- Leder skal ved endringer av ansvar eller organisatorisk tilhørighet internt i forvaltningen vurdere medarbeideres tilganger i IKT-systemene, samt sørge for eventuelle endringer i tilgangsbehov på IKT-systemene effektueres.

7. SIKKERHETSHENDELSER

- Leder skal etablere rutiner i enheten slik at sikkerhetsrelaterte hendelser håndteres og rapporteres korrekt, herunder at;
  - Sikkerhetshendelser skal alltid rapporteres til nærmeste leder.
  - Generelt gjelder at sikkerhetsbrudd sees på som mislighold av arbeidsavtalen og vil bli behandlet som personalsak.
  - Forsøk på oppslag på personer det ikke foreligger tjenstlig behov for, eller annen form for misbruk av personopplysninger skal konfronteres.
  - Ved misbruk av passord skal leder sørge for at passord blir byttet.
  - For hendelser relaterte til teknisk sikkerhet skal IKT Drift kontaktes.
  - For hendelser relatert til fysisk sikkerhet (f.eks. manglende låsing, tyveri, osv.) skal sikkerhetskoordinator kontaktes.

8. PERMISJONER ELLER ANDRE TYPER MIDLERTIDIGE ARBEIDSOPPHOLD

- Leder skal vurdere og eventuelt sørge for innlevering av nøkler/adgangskort/utlånt utstyr;
  - Unntak: dersom jobbrelaterte hensyn tilsier at nøkler/adgangskort/utlånt utstyr ikke skal leveres tilbake i permisjonstiden, kan dette avtales og dokumenteres.
- Leder skal påse at sensitiv informasjon er nedlåst og at sperring av brukerident er gjennomført.

9. AVSLUTNING AV ARBEIDSFORHOLD

- Leder skal sørge for at medarbeider har ryddet i, og eventuelt slettet og/eller makulert, dokumentasjon og filer.
- Leder skal sørge for at forvaltningens eiendeler som mobiltelefon, bærbar PC, nøkler, adgangskort ol.er innlevert.
- Leder skal sørge for sperring av brukerident **og fjerning av brukertilganger**.
- Leder skal sørge for at adgangskort sperres.

10. SIKKERHETSGRADERT INFORMASJON

- Leder skal sørge for at sikkerhetsgradert informasjon alltid forsendes i tråd med gjeldende retningslinjer for informasjonens gradering.
- Leder kan kontakte sikkerhetskoordinator for nærmere informasjon om dette.
- Den som behandler gradert informasjon skal være sikkerhetsklarert og autorisert for dette.
- Ansatte som er sikkerhetsklarert og autorisert skal undertegne særskilt taushetserklæring
  - Behandling av BEGRENSET informasjon krever ikke sikkerhetsklarering, men kun autorisasjon.
  - Behandling av KONFIDENSIELL og HEMMELIG informasjon krever både sikkerhetsklarering og autorisasjon.
- Behandling av gradert informasjon skal ikke skje i IKT systemer.
- BEGRENSET informasjon/dokumenter skal lagres i enhetens arkiv.
- KONFIDENSIELL og HEMMELIG informasjons skal arkiveres i safe som er godkjent for dette formålet, samt føres i egen postliste.

20 6. SIGNATUR

Denne side signeres, skrives ut og oppbevares i personalmappe til leder sammen med signert sikkerhetsinstruks for medarbeider.

Jeg bekrefter herved at tilleggsinstruks for leder er lest og forstått:

Sted: _____ **Dato:** _____

Navn med blokkbokstaver: _____

Signatur: _____