



Dokument-ID : IM 2008-029
Saksnummer : 15/05435-21
Sist endret : 05.07.2017
Dokumentdato: 12.12.2008
Mottakere : Alle i UDI

Instruks for personvern, IKT og sikkerhet

Til alle medarbeidere i Utlendingsdirektoratet

Instruksen for personvern, IKT og sikkerhet er en operativ instruks som inngår i UDIs internkontrollsystem. Internkontrollsystemet skal ivareta personvern- og sikkerhetskravene etter henholdsvis personopplysningsloven og sikkerhetsloven.

Denne instruksen setter krav om og gir retningslinjer for

- *ivaretagelsen av personvern og informasjonssikkerhet for våre brukere*
- *bruken av IKT i UDI*
- *sikringen av UDIs medarbeidere og lokaler*

Alle som får adgangskort til UDIs lokaler eller tilgang til personopplysninger vi forvalter, skal være kjent med disse kravene. Du bør derfor lese instruksen nøye, og jeg anbefaler deg også å lese den på nytt ved jevne mellomrom. Hvis du har spørsmål om instruksen kan du kontakte din nærmeste leder, personvernrådgiver eller sikkerhetsrådgiver i avdelingen din.

Vennlig hilsen

*Frode Forfang
direktør*

1. Om instruksen

Denne instruksjonen gir retningslinjer for adgangen til UDIs lokaler og bruken av UDIs utstyr, systemer og nettverk. Formålet med instruksjonen er å gi deg en oversikt over kravene vi stiller til deg som ansatt eller innleid konsulent (heretter kalt medarbeider), om personvern, bruk av IKT-utstyr og sikkerhet.

Som medarbeider i UDI plikter du å etterleve og forstå denne instruksjonen, samt kravene og de interne retningslinjene instruksjonen bygger på. Du plikter også å gjøre deg kjent med relevante interne retningslinjer, disse finner du i Regelverksportalen (RVP) og på UDISIA under Sikkerhet, Personvern og Varsling.

2. Oppstart av arbeidsforholdet i UDI

Som ny medarbeider i UDI skal du

- ta e-læringskurset «Grunnkurs personvern, IKT og sikkerhet» og bestå en etterfølgende test
- avgi en egenerklæring om at du har lest og gjort deg kjent med kravene i instruksjonen. Du avgir egenerklæringen i forbindelse med e-læringskurset

3. Taushetsplikt

Som medarbeider i UDI skal du

- gjøre deg kjent med innholdet i relevante interne retningslinjer og rutinebeskrivelser som omhandler taushetsplikt
- underskrive taushetserklæring
- overholde taushetsplikten, se forvaltningsloven § 13

4. Personvern

Personopplysningsloven stiller krav til når og hvordan du kan behandle personopplysninger. Alle medarbeidere har ansvar for å ivareta kravene i personopplysningsloven med tilhørende forskrift.

Hvis du har spørsmål om personvern eller behov for veiledning, ta kontakt med personvernrådgiverne i din avdeling. For nærmere informasjon om personvern og hvem som er personvernrådgiverne i avdelingene, se [udisia/verktøykassa/personvern](#).

Som medarbeider i UDI skal du

- vite hva en personopplysning er, og hva som regnes som sensitive personopplysninger, se personopplysningsloven § 2 nr. 1 og 8
- kun behandle personopplysninger i samsvar med gjeldende regelverk, se personopplysningsloven, utlendingsloven, statsborgerloven og forvaltningsloven
- kun behandle, herunder søke på, opplysninger som er nødvendige for at du skal kunne utføre arbeidsoppgavene dine (tjenstlig behov), jf. personopplysningsforskriften § 2-8 første ledd
- kun utlevere (formidle) opplysninger til andre utenfor UDI når det foreligger hjemmel i lov
- bidra til å ivareta rettighetene til brukerne våre (de registrerte), herunder UDIs informasjonsplikt og de registrertes innsynsrett, se personopplysningsloven §§ 18 og 19
- ikke behandle flere personopplysninger enn det som er nødvendig for å utføre arbeidsoppgavene dine
- sørge for at de opplysningene du behandler er korrekte og oppdaterte
- melde fra om brudd på gjeldende personvernregelverk (avvik) til nærmeste leder, personvernrådgiver i din avdeling eller benytte skjema for avviksmelding på [Udisia](#)

5. UDIs IKT-utstyr og -systemer

5.1 Bruk av UDIs utstyr

UDIs IKT-utstyr er anskaffet for arbeidsrelatert bruk og skal kun benyttes av autoriserte medarbeidere. Brukerstøtte kan til enhver tid tilbakekalle utlevert utstyr.

Som medarbeider i UDI skal du

- alltid logge inn med egen bruker i UDIs systemer og aldri låne ut egen tilgang eller ditt personlige passord til andre
- kun benytte IKT-utstyr, lagringsmedia og programvare i UDIs nettverk som er anskaffet og godkjent av brukerstøtte

- alltid låse skjermen din når du forlater kontorplassen
- alltid ha fysisk kontroll på utstyr du tar med deg utenfor UDIs lokaler
- så raskt som mulig melde fra til brukerstøtte hvis du har mistet eller blitt frastjålet bærbart utstyr
- alltid velge «Restart» på maskinen din når du går for dagen for å sikre at du får med deg den siste oppdateringen av programvare
- begrense bruk av minnepinner til tjenstlig behov
- melde tap av minnepinne med arbeidsrelatert informasjon til nærmeste leder så snart som mulig

5.2 Internett og sosiale medier

Du er aldri anonym på Internett. Alle aktiviteter generer elektroniske spor og kan spores tilbake til maskinen du sitter på.

Du skal

- være bevisst på hva du utleverer av informasjon om UDI i sosiale medier som for eksempel Facebook, Twitter, Instagram eller private blogger. Informasjonen du gir kan misbrukes
- ikke bruke ressurskrevende tjenester på Internett som for eksempel nettradio, TV og videooverføring utover tjenstlig behov
- ikke besøke nettsider med innhold som bryter med norsk lov

5.3 Bruk av UDIs e-post

Du skal kun bruke @udi.no-adressen din til jobbrelatert korrespondanse.

- Du skal ikke åpne vedlegg eller lenker i en e-post hvis du har grunn til å mistenke at de er spam, infisert med virus eller med tilsvarende skadelig innhold.
 - Hvis du mistenker virusinfeksjon, skal du øyeblikkelig ta kontakt med brukerstøtte for å begrense skadeomfanget.
- Du skal bruke et egnet saksbehandlingssystem når du utveksler taushetsbelagte og/eller sensitive personopplysninger.
- E-post er ikke et egnet saksbehandlingssystem.
- Du kan kun sende e-post med sensitivt innhold internt, det vil si til adresser som slutter med @udi.no, @asylmottak.no, @landinfo.no. Med «sensitivt innhold» mener vi sensitive personopplysninger og/eller taushetsbelagt informasjon.
- Du kan sende e-post eksternt med innhold til og med nivå BEGRENSET gjennom Nasjonalt Begrenset Nett (NBN).
- Vær oppmerksom på at adgangen til å sende fødselsnummer er særskilt regulert i personopplysningsloven § 12.

5.4 Privat bruk av UDIs IKT-utstyr og -systemer

UDIs utstyr er anskaffet for å løse de oppgavene UDI er pålagt og er UDIs eiendom og ansvar. Av sikkerhetsmessige hensyn kan UDI gjøre nødvendige tiltak for å hindre skade på virksomhetens verdier. UDI tillater likevel en begrenset privat bruk av UDIs IKT-utstyr og -systemer. Du skal holde bruken til et minimum, og spør nærmeste leder om råd dersom du er i tvil om hva som er tillatt. Du skal merke private dokumenter og filer du har lagret i mapper på ditt personlige område med «Privat».

Dersom du fordelsbeskattes for tjenesteabonnement og utlevert IKT-utstyr, er privat bruk av dette utstyret tillatt.

6. Sikkerhet

Alle medarbeidere er ansvarlige for å bidra til en god forebyggende sikkerhet gjennom å sette seg inn i og etterleve gjeldende instruksjoner, regler og prosedyrer, se nærmere veiledning på udisia/verktøykassa/sikkerhet. Hvis du har spørsmål om sikkerhet og behov for veiledning om sikkerhet tar du kontakt med sikkerhetsrådgiverne i din avdeling. Alle avvik og sikkerhetsbrudd skal meldes til nærmeste leder, sikkerhetsrådgiver eller via skjema for avviksmelding på Udisia.

6.1 Håndtering av sikkerhetsgradert informasjon

Kun de som er sikkerhetsklarerte og autoriserte for å ha tilgang til gradert informasjon skal håndtere sikkerhetsgradert informasjon og -systemer. Alle sikkerhetsklarerte og autoriserte ansatte har plikt til å sette seg inn i sikkerhetslovens bestemmelser om håndtering av sikkerhetsgradert informasjon og systemer. Dersom du kommer i kontakt med gradert informasjon som du ikke er autorisert eller klarert for å håndtere, skal du umiddelbart avlevere dette til nærmeste leder eller avdelingens sikkerhetsrådgiver.

6.2 Adgangskort og besøkende

Alle medarbeidere skal bære UDI-adgangskort eller besøkskort synlig i lokalene våre. Du skal uoppfordret vise kortet dersom noen åpner døren for deg.

- Alle besøkende skal registreres i resepsjonen og bære besøkskort synlig.
- Hvis du møter noen uten UDI-adgangskort og uten følge av andre medarbeidere, skal du straks informere vakterne om hvor du traff vedkommende med beskrivelse av personen. Alternativt kan du følge personen til vakterne.
- Hvis du mister eller blir frastjålet UDI-adgangskortet ditt skal du så raskt som mulig melde dette til vakterne i Hausmanns gate 21.
- Du må innlevere godkjent legitimasjon for å få utlevert et lånekort for dagen, hvis du har glemt UDI-adgangskortet ditt.

7. Logging av medarbeidernes bruk av IKT og arbeidsgiverens rett til innsyn

Din bruk av UDIs IKT-utstyr og fagsystemer blir logget. Loggene inneholder blant annet informasjon om brukernavn, tidspunkt, samt hva du har gjort i de ulike systemene. Ved mistanke om bruk utover det du har tjenstlige behov for vil loggene bli gjennomgått. Det blir også foretatt rutinemessige, risikobaserte søk i loggene, uavhengig av mistanke.

Dersom du har kommet i skade for å åpne en sak av andre grunner enn det som følger av ditt tjenstlige behov, skal du umiddelbart informere nærmeste leder om dette. Arbeidsgiver gjennomfører kontroll av loggene i tråd med personopplysningslovens krav om internkontroll og UDIs interne retningslinjer.

Arbeidsgiver kan, ved mistanke om mislige eller kriminelle forhold, gjennomføre innsyn i dokumentene og filene dine. Innsyn i medarbeidernes e-post og personlig filområde skal følge retningslinjene i personopplysningsforskriften §§ 9-1 til 9-5 og UDIs interne retningslinjer.

8. Brudd på instruksen

8.1 Varslingsplikt

Alle medarbeidere har en plikt til å melde fra om brudd på denne instruksen. Hvis du har mistanke om brudd skal du rapportere det til din nærmeste leder, personvernrådgiver eller sikkerhetsrådgiver, se UDIs interne retningslinjer om varsling.

8.2 Konsekvenser ved brudd på instruksen

Brudd på denne instruksen kan få konsekvenser for arbeidsforholdet ditt i UDI.

Du risikerer

- at dine tilganger til UDIs systemer blir sperret
- sanksjoner i henhold til tjenestemannslovens bestemmelser herunder oppsigelse eller avskjedigelse
- å bli politianmeldt hvis UDI mener at bestemmelser i straffeloven, sikkerhetsloven eller annet lovverk kan være overtrådt