# Sikkerhetsinstruks – leder

*<Virksomhet>* er underlagt personopplysningsloven og tilhørende krav til informasjonssikkerhet. Dette dokumentet inneholder sikkerhetsinstruks for ledere med personalansvar i *<Virksomhet>*. Denne kommer i tillegg til generelle brukerrelaterte rutiner (se dokumentene «Informasjonshåndtering», «Sikkerhetsinstruks – bruker» og «Taushetserklæring»).

## Ansettelse

### Sjekkliste for ansettelse av faste ansatte

1. Taushetserklæringen leses og underskrives av den ansatte.
2. Sikkerhetsinstruksen leses og underskrives av den ansatte.
3. Rutine for informasjonshåndtering skal leses av den ansatte.
4. Utlevere eventuelle nøkler, nøkkelkort, koder e.l.
5. Punktene 1-4 skal gjennomføres før brukertilganger gis. Leder skal deretter informere *<IT-avdelingen>* om behov for brukertilganger. Vær spesielt oppmerksom på hvor lenge det er behov for tilgangen samt nivå på tilgang. Benytt *<felles autorisasjonsskjema>* for de ulike systemene. Disse finnes på *<Virksomhets intranettsider el.l>.*

### Sjekkliste for bruk av konsulenter og andre midlertidige ansatte:

1. Taushetserklæringen leses og underskrives.
2. Sikkerhetsinstruksen skal leses og underskrives.
3. Rutine for informasjonshåndtering skal leses.
4. Dersom det er behov for autorisasjon til informasjonssystemet, skal dette avklares med systemeier, eventuelt sikkerhetsansvarlig, før autorisasjonsskjema sendes *<IT-avdelingen el.l>*.
5. Utlevere eventuelle nøkler, nøkkelkort, koder e.l.
6. Punktene 1-5 skal gjennomføres før brukertilganger gis. Ledere skal deretter informere *<IT-avdelingen>* om behov for brukertilganger. Vær spesielt oppmerksom på hvor lenge det er behov for tilgangen og nivå på tilgang.

Leder er ansvarlig for å oppbevare en kopi av underskrevet erklæring og instruks samt autorisasjons­skje­ma for alle som inngår i personalansvaret. Original autorisasjonsskjema sendes i tillegg til *<IT-avdelingen>*.

## Regelmessig verifikasjon av brukerkonti og brukertilganger

*<IT-avdelingen>* vil regelmessig sende ut oversikt over relevante definerte brukere og bruker­tilganger til lederen med personalansvar.

Lederen skal så snart som praktisk mulig etter mottak, verifisere at oversikten er korrekt, det vil si at den reflekterer ansvar og organisasjonsmessig tilhørighet. Eventuelle feil og mangler skal formidles *<IT-avdelingen>* på e-post. Lederen skal oppbevare kopi av alle meldte endringer.

## Endring av arbeidsforhold/ansvar

Ved endringer av ansvar eller organisasjonsmessig tilhørighet internt i *<Virksomhet>* skal brukerens tilganger i informasjonssystemet vurderes. *<IT avdelingen>* skal informeres om eventuelle relevante endringer i behov for tilgang på informasjonssystemene. Leder skal oppbevare kopi av alle meldte endringer.

## Hendelser med betydning for sikkerheten

Sikkerhetsrelaterte hendelser av alvorlig karakter skal rapporteres til *<Sikkerhetsansvarlig>*.

## Konsekvenser ved brudd på retningslinjene

Brudd på *<Virksomhet>s* sikkerhetsregler er å betrakte som tjenesteforsømmelse, og skal vurderes i hvert enkelt tilfelle.

## Permisjoner eller andre typer midlertidige arbeidsopphold

Lederen skal vurdere innlevering av nøkler/adgangskort/utlånt utstyr, samt påse at sensitiv informasjon er nedlåst.

## Avslutning av arbeidsforhold

Lederen skal verifisere at arbeidstaker har levert *<Virksomhet>s* eiendeler:

*<Eksempel:*

* *Mobiltelefon*
* *Bærbar PC*
* *Nøkler*
* *Adgangskort*
* *…>*

Lederen skal også:

* verifisere at arbeidstakeren har signert for levering av *<Virksomhet>s* eiendeler og rydding i dokumentasjon og filer
* gi beskjed til *<IT-avdelingen>* om sperring av brukerkonti med brukertilganger, samt oppbevare kopi av beskjed til *<IT-avdelingen>*

Sikkerhetsinstruksen er lest og akseptert

Sted og dato: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Navn (blokkbokstaver): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signatur: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_