



# *Informasjonssikkerhet*

## *Sikkerhetsinstruks*

for

**BØ KOMMUNES**

**MEDARBEIDERE**

Versjon 5.0

## INNHOOLD

<b>INNHOOLD</b> .....	<b>2</b>
<b>DEL 1 – DEFINISJONER</b> .....	<b>3</b>
<b>DEL 2 – GENERELLE KRAV</b> .....	<b>4</b>
1. INNLEDNING .....	4
2. ANSVAR OG MYNDIGHET .....	4
3. INNLEID PERSONELL .....	5
4. INTERNETT OG SOSIALE MEDIA .....	5
<b>EKSEMPLER PÅ AKSEPTABEL BRUK AV INTERNETT:</b> .....	<b>6</b>
<b>INTERNETTETS E-POST</b> .....	<b>7</b>
<b>LOVKRAV</b> .....	<b>10</b>
1. SPESIFIKE LOVKRAV TIL INFORMASJONSSIKKERHET .....	10
2. VIKTIGE UTRAG FRA LOVENE .....	10
AVVIKSBEHANDLING .....	10
“SNOKING” I JOURNALER .....	11
INNSYN I E-POST .....	12
<b>DEL 3 SPESIELLE KRAV FOR HELSE, OMSORGS- OG SOSIALSEKTOREN</b> .....	<b>13</b>

### 1. DEFINISJONER (POL § 2)

#### A. PERSONREGISTER:

registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen.

#### B. PERSONOPPLYSNINGER:

opplysninger og vurderinger som kan knyttes til en enkeltperson

#### C. BEHANDLING AV PERSONOPPLYSNINGER:

enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

#### D. REGISTRERT:

den som en personopplysning kan knyttes til.

#### E. SAMTYKKE:

en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv.

#### F. SENSITIVE PERSONOPPLYSNINGER:

Opplysninger om:

- rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning.
- at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
- helseforhold
- seksuelle forhold
- medlemskap i fagforeninger

### 1. INNLEDNING

Denne instruksen gjelder for bruk av foretakets IKT-system. Med "IKT-system" forstås maskiner, arbeidsstasjoner, skrivere, programmer, data, flyttbare lagringsmedia, utskrifter m.v. som benyttes av eller stilles til disposisjon av foretaket, inklusive alle former for nettverk og de systemene som man får tilgang til gjennom slike nettverk. Reglene gjelder for ansatte, studenter og andre som får tilgang til foretakenes IKT-system, heretter kalt bruker. Brukeren plikter å holde seg informert om den til enhver tid gjeldende instruks.

Kommunen's rolle i samfunnet innebærer en naturlig forpliktelse til å holde et høyt etisk nivå og sikre riktig kvalitet på sine primæroppgaver. Kommunen's drift og organisering medfører at sensitiv opplysninger behandles i mange ledd. Myndighetene har derfor fastsatt et regelverk for kontroll og sikkerhet som krever systematisk oppfølging.

De overordnede mål for informasjonssikkerhetsarbeidet for kommunen er å oppnå høy grad av:

- Tilgjengelighet – er det tilgjengelig når du trenger det
- Konfidensialitet – opplysninger skal ikke eksponeres for uvedkommende
- Integritet – sikre informasjon mot utilsiktet endring

Det betyr at de data som vi registrerer i våre datasystemer skal være korrekte, de skal være tilgjengelige når det er behov for dem og de skal være beskyttet mot uvedkommende.

### 2. ANSVAR OG MYNDIGHET

Rådmannen har det overordnede ansvaret for at behandling av personopplysninger i kommunen, er i samsvar med personopplysningsloven (POL).

Enhetsleder er behandlingsansvarlig i sin resultatenhets.

Hun/han er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler, herunder systemer og rutiner/prosedyrer som skal etableres og brukes ref pol § 2 pkt 4 for å oppfylle de aktuelle lovkrav.

Den enkelte saksbehandler(bruker) som behandler personopplysninger på oppdrag fra behandlingsansvarlig enhetsleder, er databehandler ref pol § 2 pkt 5. Hun/han er

ansvarlig for å sette seg inn i og behandle opplysningene i samsvar med gjeldende lovverk og de rutiner enhetsleder som behandlingsansvarlig har godkjent.

Lærlinger, elever og studenter i praksis er ansvarlig for å sette seg inn i enhetens rutiner for behandling av personopplysninger. Studentens behandling av personopplysninger skal kun skje i opplæringsøyemed og under veiledning av dataansvarlig saksbehandler eller enhetsleder som behandlingsansvarlig.

Forholdet mellom personopplysningsloven og særlovgivning på tjenesteområdene. Dersom det i særlovgivning stilles skjerpede krav til behandling av personopplysninger, skal enhetsleder sikre at det etableres rutiner som ivaretar disse kravene.

Alle som utfører arbeide for kommunen, ansatte, midlertidig ansatte og oppdragstakere har lovbestemt taushetsplikt. Plikten gjelder både i arbeidet og privat, og den varer også etter avsluttet arbeidsforhold i kommunen.

Lederen for den enkelte avdeling/enhet/kontor har ansvar for å opprettholde en tilfredsstillende informasjonssikkerhet innenfor sitt ansvarsområde.

Den enkelte medarbeider har ansvar for å sette seg inn i informasjonssikkerhetsreglene og følge disse.

God informasjonssikkerhet oppnås gjennom den enkelte ansattes holdning og årvåkenhet, og ved at den enkelte ansatte kan vise ansvar for informasjonssikkerheten og følge gjeldende retningslinjer innenfor sitt arbeidsområde.

---

### 3. INNLEID PERSONELL

Innleid personell skal behandles som besøkende og hentes og følges under arbeidet spesielt i områder hvor sensitiv informasjon eksponeres, med mindre den enhetsleder som har ansvaret for arbeidet gir dispensasjon. Ikke under noen omstendighet skal teknikere og andre eksterne fritt kunne oppholde seg inne på maskinrom (tekniske rom, datarom, osv.), De skal alltid ha følge av fast ansatt personell. (Unntaket er autorisert personell som har underskrevet taushetsløfte)

For å få tilgang til kommunen's datasystemer, må alle ansatte, oppdragstakere og midlertidig ansatte gis nødvendige autorisasjoner gjennom sin enhetsleder, og taushets- og arbeids-avtale må undertegnes.

---

### 4. INTERNETT OG SOSIALE MEDIA

Det er ikke tillatt å koble internett-forbindelser opp mot vårt nettverk uten særskilt tillatelse. Kommunen behandler og oppbevarer konsesjonsbelagt informasjon og informasjon som er underlagt taushetsplikt. Kommunen skal behandle og sikre data

etter de vilkår som konsesjonen setter og etter lov og forskrifter gitt av offentlig myndigheter, samt vår taushetsplikt og kommunen's egne krav til sikkerhet.

Det er ikke tillatt å benytte internett som kanal for å utveksle sensitive data som ikke skal være alminnelig kjent. Under visse forhold kan utveksling av data utføres, men da i samråd med IKT-avdeling / sikkerhetsansvarlig.

Internett kan være meget nyttig kanal for informasjonsutveksling, men du må huske på at internett er en åpen kanal hvor det er mulig for uvedkommende å få tilgang til den informasjon som du utveksler. Det kan være mulig for uvedkommende å lese, gjøre endringer eller på annen måte misbruke data som overføres på internett

#### EKSEMPLER PÅ AKSEPTABEL BRUK AV INTERNETT:

- Å oppdatere seg faglig gjennom tilgjengelige nettmedia som lovdata, offentlige utredninger, biblioteksregister, nyheter og andre relevante kilder som f.eks. medisinske oppslagsverk/ databaser.
- Å utveksle ikke sensitiv-faglig informasjon med kollegaer gjennom e-post.

#### EKSEMPLER PÅ UAKSEPTABEL BRUK:

- Å laste ned programvare og spill fra nettet og med mindre dette på forhånd er godkjent av IKT – avdelingen
- Installasjon av programvare, med mindre det er godkjent av IKT – avdelingen.
- Å laste ned pornografi, volds- og rasistisk prega materiale eller annet materiale som kan virke usømmelig
- Å utveksle personopplysninger og andre opplysninger av fortrolig karakter.
- 

#### ANSATTES BRUK AV SOSIALE MEDIA

Huskeregler for hvordan ansatte kan bruke sosiale medier til for eksempel faglige diskusjoner:

1. Vær gjerne aktiv i faglige diskusjoner.
2. Opptre på samme måte som du ville gjort ellers i hverdagen. Bruk sunn fornuft.
3. Vær bevisst på rollen din som ansatt i kommunen.

4. Vurder om du skal ha kontakt med elever/brukere/pårørende i sosiale medier som for eksempel Facebook eller MSN. I så fall, tenk på hvordan du opptrer.
5. Ansatte har ytringsfrihet, men taushetsplikten gjelder også i de sosiale mediene.
6. Vær åpen om hvor du jobber.
7. Presiser at du ytrer deg som privatperson og ikke på vegne av kommunen.
8. Henvendelser direkte til kommunen besvares av administratorer på de forskjellige kontoene.
9. Husk at Internett er permanent, det kan være vanskelig å slette det du har sagt.
10. Er du i tvil, send en e-post til postmottaket.
11. Husk – det forventes at svaret kommer raskt.

*(Teksten er lånt av Trondheim Kommune)*

## INTERNETTETS E-POST

Elektronisk post, E-post, kan sendes internt i kommunen og til andre brukere på Internett.

Å sende/motta E-post er forbundet med følgende risiko:

- **Sendingene kan bli tappet underveis**
- **Opphavsmannen kan forfalske sin identitet og adresse**
- **Meldingen/dokumentet kan forfalskes (endres under veis)**
- **Meldingen kan lett sendes til feil adressat**

Ved sending av E-post (på internett) internt innenfor og utenfor kommunen skal alle personopplysninger anonymiseres . Det skal aldri sendes sensitive opplysninger (heller ikke anonymiserte) verken innenfor eller utenfor kommunen.

**Sensitive opplysninger skal ikke sendes via telefaks.**

---

## 5. SIKKERHET OG ORDEN PÅ KONTORET

- La ikke sensitiv/fortrolig informasjon ligge å flyte på skrivebordet, skrivere etc.
- Kast ikke sensitive/fortrolige dokumenter, usb-penner, CD'er etc. i papirkurven. Makuler dem!
- Uvedkommende skal ikke ha tilgang til steder hvor datautstyr, kommunikasjonsutstyr, skrivere, telefakser o.l. er plassert, uten i følge med ansatt
- Den enkelte medarbeider skal aktivt bidra til at det ikke blir liggende igjen personopplysninger på skrivere og kopimaskiner som eksponeres for uvedkommende.

---

## 6. ANDRE KRAV TIL DEN ENKELTE BRUKER

- a) Ved all bruk av systemet skal brukeren identifisere seg ved å oppgi eget brukernavn og passord.
- b) En bruker har plikt til å følge anvisninger om bruk av systemet og tjenester knyttet til systemet. En bruker skal sette seg inn i aktuelle bruksanvisninger og dokumentasjon, for på den måten å hindre feilbruk eller driftsforstyrrelser.
- c) Når arbeidsplassen forlates, skal brukeren alltid logge seg av systemet eller låse arbeidsstasjonen. Dette bidrar til å hindre at ikke-autoriserte får innsyn i IKT-systemene.
- d) Brukernavnet er strengt personlig. Bruk eller forsøk på bruk av andre brukeres brukernavn og/eller passord ved pålogging er ikke tillatt. Det er ikke tillatt å utgi seg for å være en annen person ved bruk av foretakets IKT-systemer.
- e) Passordet skal være på 8 eller flere tegn, og bør inneholde både tall og bokstaver for å gjøre det vanskeligere å avsløre passordet for uvedkommende. Navn, brukernavn, fødselsdato eller lignende skal ikke benyttes. Husk at passordet er din nøkkel til de opplysningene som finnes på foretaket.
- f) En bruker skal beskytte passord og liknende sikkerhetslementer slik at disse ikke blir kjent for andre. Dersom brukeren har mistanke om at slikt er blitt kjent, skal bruker sørge for at passord m.v. skiftes umiddelbart.
- g) En bruker skal forhindre at ikke-autoriserte personer får tilgang til bruk av systemet eller tilgang til rom hvor utstyr er tilgjengelig.
- h) En bruker skal rapportere forhold som kan ha betydning for systemets sikkerhet eller integritet i henhold til gjeldende rutine for melding av avvik. Alvorlige hendelser eller tilstander rapporteres i tillegg umiddelbart til Sikkerhetsansvarlig.

- i) Det er ikke tillatt å importere programmer fra eksterne nett uten at dette er godkjent.
- j) Ved opphør av ansettelsesforhold skal brukeren rydde sitt reserverte område. Skjer ikke dette vil IT-avdelingen slette filer og fjerne brukernavnet. For øvrig henvises det til personalrutinene vedrørende avvikling av arbeidsforhold.
- k) Det er ikke anledning til å lagre sensitive personopplysninger på bærbar maskiner med mindre spesiell tillatelse er gitt av behandlingsansvarlig i samråd med sikkerhetsansvarlig.

Alle som har bærbar pc må jevnlig logge maskinen på kommunens nettverk for å oppdatere antivirusprogram. Den som disponerer bærbar pc skal ikke fjerne eller deaktivere antivirusprogramvare som er installert på pc-en.

Har den ansatte mistanke om at det kan være virus eller annen skadelig programvare på utstyret, skal den ansatte straks levere datamaskinen til IT-avdelingen. Maskinen skal ikke kobles inn i kommunens nett.

## **HUSK: SIKKERHET BEGYNNER MED DEG!!**

---

**Informasjonssikkerhet angår alle, og det er ditt ansvar!  
Husk taushetsplikten din!**

### 1. SPESIFIKE LOVKRAV TIL INFORMASJONSSIKKERHET

Her er en rekke lover som alle stiller krav til informasjonssikkerhet. De to viktigste lovene i så måte er **personopplysningsloven med forskrift og helseregisterloven**. Nedenfor er det listet opp en rekke lover som i større eller mindre grad stiller krav til informasjonssikkerheten. Enhetsleder vil kunne gi deg veiledning i hvilke lover som er gjeldende for din enhet.

Barnevernsloven	Sosialloven	Åndsverkloven
Bokføringsloven m/ forskrift	Kommuneloven	Arkivloven/m forskrift
Lov om etablering og gjennomføring av psykisk helsevern	Forvaltningsloven	Lov om helsemessig og sosial beredskap
Lov om pasientrettigheter	eForvaltningsforskriften	Lov om helsepersonell
Lov om arbeidervern og arbeidsmiljø m.v.	Lov om retten til oppfinnelser som er gjort av arbeidstakere	Pasientrettighetsloven

### 2. VIKTIGE UTDRAG FRA LOVENE

#### AVVIKSBEHANDLING

*POF § 2-6 Avvik (POF=personopplysningsforskriften)*

*Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik.*

*Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentakelse.*

*Dersom avviket har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet varsles.*

*Resultatet fra avviksbehandling skal dokumenteres.*

Et viktig middel for å forbedre sikkerheten er å føre avviksmelding når en kommer over forhold som må rettes på når det gjelder sikkerhet. Avviksmeldingen skal leveres enhetsleder.

---

## “SNOKING” I JOURNALER

Fra 9. mai 2009 ble det straffbart ”å snoke” i journaler

Hittil har snoking bare vært underlagt tjenstlige reaksjoner. Nå risikerer ansatte som bryter med brudd på reglene om snikkikking opptil 3 måneders fengsel.

Alle ansatte med tilgang til pasientopplysninger må derfor være om mulig enda mer bevisst på at snoking ikke kan tolereres.

---

### HELSEREGISTERLOVEN LYDER:

§ 13a. Forbud mot urettmessig tilegnelse av helseopplysninger

Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helseopplysninger som behandles etter denne loven uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift.

§ 34. Straff

Den som forsettlig eller grovt uaktsomt overtrer § 13 a, straffes med bøter eller fengsel i inntil tre måneder.

---

### HELSEPERSONELLOVEN LYDER:

§ 21a. Forbud mot urettmessig tilegnelse av taushetsbelagte opplysninger:

Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte opplysninger som nevnt i § 21 uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift.

§ 67. Straff

Den som forsettlig eller grovt uaktsomt overtrer eller medvirker til overtredelse av bestemmelser i loven eller i medhold av den, straffes med bøter eller fengsel i inntil tre måneder. Offentlig påtale finner sted hvis allmenne hensyn krever det eller etter begjæring fra Statens helsetilsyn.

---

## INNSYN I E-POST

Bestemmelsene ble vedtatt 28. januar 2009, og inngår som nytt kap. 9 i personopplysningsforskriften.

Bestemmelsene gjelder for innsyn i arbeidstakers e-postkasse mv. Formuleringen omfatter innsyn i eventuelle e-postkasser den ansatte har fått i virksomheten til bruk i sitt arbeide, men også innsyn i og gjennom søking av arbeidstakerens personlige område i virksomhetens datanett og innsyn i annet elektronisk utstyr. Forutsetningen er at det er arbeidsgiver som eier utstyret, og at arbeidstakeren har fått utlevert utstyret eller tilgang til det for bruk i sitt arbeid.

Bestemmelsene gjelder dermed ikke for innsyn i utstyr som den ansatte selv eier, selv om dette fra tid til annen benyttes i arbeidet ved virksomheten. Arbeidsgiver vil som hovedregel være avskåret fra innsyn i slikt privateid utstyr.

[Les forskriften her \(hos Lovdata, nytt vindu\)](#)

---

### I FØLGENDE SITUASJONER KAN INNSYN VÆRE AKTUELT:

Når det er nødvendig for å ivareta den daglige driften.

Når det er nødvendig for å ivareta andre berettigede interesser ved virksomheten.

Ved begrunnet mistanke om at bruk av e-postkassen medfører grovt brudd på de plikter som følger av arbeidsforholdet.

Ved begrunnet mistanke om at arbeidstakers bruk av e-postkassen kan gi grunnlag for oppsigelse eller avskjed.

---

### RÅD TIL ARBEIDSTAKERE

- Begrens de private aktivitetene på arbeidsgivers datasystem. Datasystemet er ment for å utføre arbeidsoppgaver.
- Prøv å unngå korrespondanse som ikke er jobberelatert via e-posten på jobben.
- Merk e-poster som er private med "privat" i emnelinjen og/eller lagre disse i et mappesystem som tydelig viser at innholdet er privat.
- Fravær registrer deg ved både planlagt og utilsiktet fravær
- Send arkivverdig materiale til postmottaket

### Norm for informasjons- sikkerhet

Norm for informasjonssikkerhet i **helse-, omsorgs- og sosialsektoren** (Normen) er et omforent sett av krav til informasjonssikkerhet, basert på lovverket. Normen er utarbeidet av representanter for helsesektoren, bl.a. Legeforeningen, Sykepleierforbundet, Tannlegeforeningen, KS, Apotekerforeningen og regionale helseforetak.

Normen omfatter alle krav som må tilfredsstilles for å oppfylle lov- og forskriftskrav til informasjonssikkerhet i helsesektoren. Normen kan også stille strengere krav enn det som følger av lovverket. **Alle aktører i helsesektoren som er tilknyttet Norsk Helsenett er avtalerettslig forpliktet til å følge Normen.**

Normen består av en Normtekst og en rekke fakta ark. Normteksten er dekket i "Håndboken for informasjonssikkerhet" tilhørende kommunen. I tillegg er det utformet en rekke fakta ark som er egnet som veiledning, hvorav 12 har brukere som målgruppe.

Nedenfor er det listet opp de fakta ark som er rettet til dere som brukere (4 I alt) og som ikke er dekket i denne instruksjonen så langt.

[Se normen og tilknyttet informasjons- og faktaark her \(nytt vindu\)](#)

Fakta ark	Formål og fokusområder
<a href="#">15</a> <a href="#">Hendelsesregistrering og oppfølging</a>	<p>Formålet med hendelsesregistrering og oppfølging av hendelsesregistre er å:</p> <ul style="list-style-type: none"> <li>• gi oversikt over autorisert bruk av helse- og personopplysninger i virksomheten</li> <li>• sette virksomheten i stand til å avdekke uautorisert bruk, eller forsøk på uautorisert bruk, av helse- og personopplysninger</li> <li>• forebygge, avdekke og forhindre gjentakelse av sikkerhetsbrudd i informasjonssystemene</li> <li>• legge til rette for pasient/brukers rett til innsyn i hendelsesregistre, slik at vedkommende gis mulighet til å ivareta egne rettigheter</li> <li>• legge til rette for ansattes rett til innsyn i opplysninger som er lagret om vedkommende i hendelsesregisteret</li> </ul>
	<p><b>Noen punkter du som bruker må ha fokus på:</b></p> <p>a) Alle forsøk på uautorisert bruk av behandlingsrettede helseregistre og fagsystemer</p> <p>b) All bruk av nødrettstilgang skal dokumenteres og hvert enkelt tilfelle skal følges opp som et avvik for å påse at begrunnelse er relevant</p> <p>c) Ved brudd på regler om at sensitive personopplysninger ikke skal utleveres ved hjelp av epost skal regelbruddet behandles som avvik og personalmessige konsekvenser vurderes</p>
<a href="#">41 Skadereparasjon når data har blitt utilsiktet utlevert</a>	<p>Håndtere utilsiktet utlevering av helse- og personopplysninger på en korrekt måte samt gi ansatte opplæring i håndtering av utilsiktet utlevering.</p> <p>Hele fakta arket kommer til anvendelse</p>
<a href="#">45 Personvern og informasjonssikkerhet – en kort orientering for det enkelte helse- og sosialpersonell i kommuner</a>	<p>Bidra til bevisstgjøring om at den enkelte medarbeider møter personvernsspørsmål i arbeidshverdagen og at krav til personvern og informasjonssikkerhet skal følges.</p> <p>Hele fakta arket kommer til anvendelse</p>
<a href="#">50 Innsyn i hendelsesregistre</a>	<p>Sikre den registrertes rett til innsyn i hendelsesregistre fra behandlingsrettet helseregister og fagsystem.</p> <p>Hele fakta arket kommer til anvendelse</p>