# Informasjonssikkerhet

Retningslinjer for behandling av personopplysninger og annen informasjon underlagt taushetsplikt

STAVANGER KOMMUNE

## For hvem?

Retningslinjene omfatter alle som har tilgang til kommunens IT-systemer.

## Hvorfor?

**Informasjonssikkerhet** trenger vi for at uvedkommende ikke skal få tilgang til personopplysninger om brukere av kommunens tjenester, eller annen informasjon underlagt taushetsplikt.

**Retningslinjer for informasjonssikkerhet** skal være et redskap slik at vi sammen kan oppbevare og behandle informasjon på en forsvarlig måte.

## Definisjoner

**Personopplysninger** er opplysninger og vurderinger som kan knyttes til enkeltpersoner.

**Sensitive personopplysninger** er informasjon
- som omfattes av forvaltningslovens og særlovenes bestemmelser om taushetsplikt
- som røper et klientforhold
- om rasemessig eller etnisk bakgrunn eller politisk, filosofisk eller religiøs oppfatning
- om en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
- om helseforhold og andre forhold som omfattes av helsepersonellovens regler om taushetsplikt
- om seksuelle forhold

**Behandling av personopplysninger** er enhver bruk av personopplysninger som for eksempel innsamling, registrering, sammenstilling og lagring, utlevering eller kombinasjon av bruksområder.

## Personopplysningslovens § 13 Informasjonssikkerhet

Den behandlingsansvarlige og databehandleren skal sørge for tilfredstillende informasjons-sikkerhet med hensyn til ***konfidensialitet***, ***integritet*** og ***tilgjengelighet*** ved behandling av personopplysninger.

## Personopplysningslovens § 14 Internkontroll

Den behandlingsansvarlige skal etablere og holde ved like planlagte og systematiske tiltak som er nød-vendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplys-ningenes ***kvalitet***.

# Konfidensialitet

**Med "*konfidensialitet*" menes at personopplysninger og annen informasjon underlagt taushetsplikt må være sikret mot at uvedkommende får kjennskap til opplysningene.**

IT-systemene som benyttes i kommunen inneholder store mengder personopplysninger. Du er medansvarlig for at opplysningene behandles på en slik måte at uvedkommende ikke får tilgang til dem.

Du er pålagt taushetsplikt gjennom lov og kommunalt reglement. Denne plikten til å beskytte informasjon må videreføres når du behandler informasjon elektronisk.

## Din arbeidsplass

- Sett deg inn i de rutiner og regler som gjelder for din arbeidsplass, særlig med tanke på tilgang til systemer, adgang til bygget/lokalene, besøk fra brukere, makulering, arkivering og hvordan du skal forholde deg ved feilsituasjoner på IT-systemene.

- Plasser deg selv og skjermen din på en slik måte at uvedkommende ikke kan se hva som står på skjermen. Dette gjelder både for de som tilfeldig går forbi arbeidsplassen din (inne og ute), og de som er på besøk/samtaler med deg.

- Besøkende skal som hovedregel hentes og følges.

- Sørg for at uvedkommende ikke får tilgang til pc-en din. **Aktiver skjermbeskytteren hver gang du forlater arbeidsplassen!**

- Logg deg ut av alle systemer og skru av Pc-en ved arbeidsdagens slutt.

- Hvis mulig: lås kontordøren når du forlater arbeidsplassen, og forsikre deg om at dører som skal være låst er låst.

## Dokumenter og utskrifter

- La aldri personopplysninger eller annen informasjon underlagt taushetsplikt ligge åpent tilgjengelig slik at uvedkommende får tilgang eller innsyn. Legg papirer, brev og notater i skuffer eller skap som du låser når du forlater arbeidsplassen for lengre tid. Oppbevar nøklene forsvarlig!

- La ikke utskrifter bli liggende på skriver eller telefaks! Hent utskriftene dine umiddelbart!

- Utskrifter som gjelder enkeltpersoner skal arkiveres i den fysiske klientmappen / pasientjournalen så snart som mulig. Jf. arkivreglement(ene) som gjelder for din arbeidsplass.

- Utskrifter som gjelder flere personer (rapporter og lister) skal oppbevares i låsbart skap og makuleres når de ikke lenger er nødvendige for formålet.

- Overflødige utskrifter og lagringsmedier (disketter/CD'er) skal alltid makuleres.

## E-post og telefaks

- Elektronisk post (Notes-mail el. tilsvarende) og telefaks skal ikke brukes til formidling av sensitive personopplysninger. Klient/pasient/brukernavn eller personnummer skal aldri brukes i e-post/telefaks!

- Begrens antall mottakere og innhold ved bruk av elektronisk post og slett jevnlig i din inn- og utboks.

## Internett og kommunenett

- Når ansatte får tilgang til Internett på arbeidsstedet skal dette bare benyttes av den enkelte arbeidstaker i jobbsammenheng.

- Systemet skal benyttes på en lovlig og etisk forsvarlig måte.

- Last aldri ned programvare fra Internett.

- Informasjon eller materiell som kan virke krenkende eller utilbørlig, skal under ingen omstendighet nedlastes, lagres eller formidles.

- Kommunens IT-nettverk skal ikke under noen omstendigheter endres av andre enn IT-avdelingen. Med dette menes for eksempel tilkobling av nytt utstyr til nettverket, flytting/endring av eksisterende nettverksutstyr, tilkobling til andre nettverk o.l.

- Det er ikke tillatt å installere programvare på eget initiativ på kommunens pc-er, eller endre oppsettet på pc-ene. Programvare og oppsett skal alltid distribueres elektronisk fra IT-avdelingen. Eventuelle unntak fra dette skal avklares med IT-avdelingen.

## Passord

Alle som benytter kommunens IT-systemer i sitt arbeid skal ha personlig(e) passord og brukernavn.

- Lån aldri ut brukernavn og passord til andre!

- Lån aldri andres brukernavn og passord!

- Ha aldri passord(ene) nedskrevet på arbeidsplassen slik at andre kan lese dem!

## Personopplysningslovens § 11:
## Grunnkrav til behandling av personopplysninger

Den behandlingsansvarlige skal sørge for at personopplysningene som behandles

a) bare behandles når dette er tillatt etter § 8 og § 9,
b) bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet,
c) ikke brukes senere til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker,
d) er ***tilstrekkelige og relevante*** for formålet med behandlingen, og
e) er ***korrekte og oppdatert***, og ikke lagres lenger enn det som nødvendig ut fra formålet med behandlingen, jf. §§ 27 og 28

# Integritet

**Med "*integritet*" menes at personopplysninger og annen informasjon underlagt taushetsplikt må være sikret mot utilsiktet eller uautorisert endring eller sletting.**

Det er IT-avdelingens ansvar å sørge for at det iverksettes sikkerhetstiltak som forhindrer at uvedkommende kan endre eller slette opplysninger som er registrert.

Når du behandler personopplysninger er det ditt ansvar å kontrollere at opplysninger du registrerer knyttes til riktig person, og at du ikke endrer eller sletter personopplysninger på feil person.

# Tilgjengelighet

**Med "*tilgjengelighet*" menes at personopplysninger og annen informasjon underlagt taushetsplikt som skal behandles av autorisert personell, er tilgjengelig til den tid og på det sted der det er behov for opplysningene.**

Den enkelte medarbeider skal bare ha tilgang til personopplysninger som er nødvendig ut ifra ***tjenstlig behov***, dvs. opplysninger som er nødvendig for å yte hjelp og/eller utføre saksbehandling og administrasjon.

Det er IT-avdelingens ansvar å sørge for at du har tilgang til de IT-systemene du trenger i ditt arbeid.
Nærmeste leder bestiller nødvendige tilganger i god tid før nye medarbeidere begynner, og melder fra om opphør eller endring av tilgang når medarbeidere slutter eller endrer arbeidssted/arbeidsområde.

Dersom du trenger tilgang til nye systemer, kontakt din nærmeste leder.

Har du glemt nettverkspassordet ditt, eller på annen måte ikke får tilgang til systemer du vanligvis har tilgang til, kontakt IT-avdelingens kundesenter på tlf. (5150) 8080.
Har du glemt passordet til fagsystemet du bruker, kontakt din nærmeste leder.

# Kvalitet

**Med *"kvalitet"* menes at personopplysninger og annen informasjon underlagt taushetsplikt må være korrekt, oppdatert, samt relevant og tilstrekkelige som grunnlag for saksbehandling og tjenesteytelse.**

Når du behandler personopplysninger er det ditt ansvar å påse at du registrerer ***tilstrekkelig*** opplysninger sett i forhold til hva saken gjelder. Det er likevel bare opplysninger som er ***relevante*** for formålet som skal registreres.

Du har også ansvar for å påse at de personopplysninger du registrerer er ***korrekte,*** og at opplysninger som er registrert tidligere blir ***oppdatert*** fortløpende.

# Avvikshåndtering

**Med *"avvik"* menes enhver håndtering av personopplysninger og annen informasjon underlagt taushetsplikt som ikke utføres i henhold til gjeldende regelverk, retningslinjer og/eller prosedyrer, samt andre sikkerhetsbrudd.**

Alle avvik skal rapporteres til nærmeste leder. Den som oppdager et avvik er ansvarlig for å melde fra om dette uavhengig av hvem eller hva som har forårsaket avviket. Alvorlige avvik skal meldes leder umiddelbart.

***Alvorlig avvik*** er avvik som har ført til/kunne ha ført til fare for liv og helse eller brudd på taushetsplikten.

Leder skal iverksette tiltak for å stanse et pågående avvik og forhindre at tilsvarende skjer på ny. Alvorlige avvik skal meldes til overordnet leder.

# Sikkerhetsregler

1 Uvedkommende skal ikke ha tilgang til sensitive personopplysninger eller annen informasjon underlagt taushetsplikt. ***Du*** er ansvarlig for å opptre på en slik måte at dette ikke skjer.

2 Du har lovpålagt taushetsplikt. Plikten til å beskytte informasjon gjelder også når du behandler informasjon elektronisk.

3 Personopplysninger du registrerer skal være tilstrekkelige og relevante for formålet og korrekte og oppdaterte.

4 La aldri personopplysninger ligge åpent tilgjengelig slik at uvedkommende får tilgang eller innsyn.

5 Hent utskrifter og telefakser umiddelbart. Makuler overflødige utskrifter.

6 E-post og telefaks skal ***ikke*** brukes til formidling av sensitive personopplysninger.

7 Plasserer deg selv og skjermen din på en slik måte at uvedkommende ikke kan se hva som står på den.

8 Aktiver skjermbeskytteren hver gang du forlater arbeidsplassen.

9 Lån aldri ut ditt brukernavn og passord til andre.

10 Logg deg ut av alle systemer og skru av PC-en ved arbeidsdagens slutt.

11 Forsikre deg om at dører som skal være låst er låst.

12 Besøkende skal som hovedregel hentes og følges.

13 Sett deg inn i rutiner og regler for informasjonssikkerhet ved din arbeidsplass.

14 Rapporter alle sikkerhetsbrudd til nærmeste leder.

STAVANGER KOMMUNE

Postboks 8001 - 4068 Stavanger
Telefon 51 50 70 90.
E-post: postmottak@stavanger.kommune.no
www.stavanger.kommune.no