

 Norm for informasjonssikkerhet www.normen.no	Utgitt med støtte av: 
<h2>Retningslinjer for daglig informasjonssikkerhet</h2>	<b>Støttedokument</b> <b>Faktaark nr 27</b> Versjon: 2.1 Dato: 15.12.2010

<b>Målgruppe</b>  Dette faktaarket er spesielt relevant for:	<input type="checkbox"/> Leverandør <input type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder / sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input checked="" type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
<b>Ansvar</b>	Virksomhetens ledelse er ansvarlig for at alle medarbeidere er kjent med og følger retningslinjer for informasjonssikkerhet. Den enkelte medarbeider har ansvar for å etterleve virksomhetens retningslinjer for informasjonssikkerhet.		
<b>Gjennomføring</b>	Retningslinjer for daglig informasjonssikkerhet må følges opp kontinuerlig.		
<b>Formål</b>	Alle medarbeidere skal opptre på en slik måte i det daglige at de ivaretar god informasjonssikkerhet i virksomheten.		
<b>Omfang</b>	Alle virksomheter skal ha retningslinjer for daglig informasjonssikkerhet. Omfanget av retningslinjene må tilpasses virksomhetens type og størrelse.		
<b>Hjemmel</b>	<ul style="list-style-type: none"> <li>• Personopplysningsloven § 13</li> <li>• Helseregisterloven § 16</li> <li>• Personopplysningsforskriften kapittel 2</li> </ul>		
<b>Referanser</b>	Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet		

Nr.	Handling/Utførelse
<b>1.</b>	<b>Retningslinjer for behandling av helse- og personopplysninger</b> <ul style="list-style-type: none"> <li>- Utskrift med helse- og personopplysninger skal kun skrives ut på skriver som står i lukket område. Alternativt kan skriver sikres med for eksempel PIN-kode eller kort</li> <li>- Utskrift med helse- og personopplysninger skal ikke forbli uavhentet på skriver</li> <li>- Medarbeider må ivareta generell orden og sikkerhet på eget kontor (låse ned papirer med helse- og personopplysninger mv.)</li> <li>- Det skal ikke være innsyn til skjermer eller papirer som inneholder helse- og personopplysninger</li> <li>- Papir med helse- og personopplysninger skal oppbevares slik at uvedkommende ikke får tilgang til opplysningene. Det anbefales å benytte låsbart skap for oppbevaring</li> <li>- Papir med helse- og personopplysninger som skal kastes skal makuleres</li> </ul>
<b>2.</b>	<b>Retningslinjer for bruk av IKT-utstyr</b> <ul style="list-style-type: none"> <li>- Skjermbeskytter m/passord skal brukes på PC uten tilsyn (for eksempel i vaktrom)</li> <li>- Det skal vises stor aktsomhet med bruk av Internett og e-post på PC som er tilkoblet datanettverk hvor helse- og personopplysninger blir behandlet</li> <li>- Trådløse nettverk skal kun benyttes etter at IKT-avdelingen har sikret og godkjent nettverkene på en tilstrekkelig måte</li> <li>- Installasjon av programvare skal kun skje etter godkjenning av IKT-avdelingen</li> <li>- Ved tilkobling av eksterne enheter (minnepinne og lignende) til PC/datanettverk skal minnepinne, o.l. skannes for ondsinnet programvare før overføring til PC og datanettverk</li> <li>- Antivirusprogramvare skal være installert og aktivert på PC hvor det lagres og behandles helse- personopplysninger. Tilsvarende skal brannmur være installert og aktivert på PC og/eller datanettverk med tilgang til Internett</li> <li>- Passord skal ikke skrives ned eller oppbevares på en slik måte at det kan gjøres tilgjengelig for uvedkommende</li> <li>- Autorisert bruker av informasjonssystemet skal ikke søke etter annen informasjon enn det brukeren er autorisert for og har behov for i den aktuelle arbeidssituasjonen</li> </ul>

Nr.	Handling/Utførelse
3.	<p><b>Retningslinjer for organisatorisk informasjonssikkerhet</b></p> <ul style="list-style-type: none"> <li>- Virksomheten skal ha prosedyrer for håndtering av leverandører og annet eksternt personale som får tilgang til områder hvor helse- og personopplysninger blir behandlet</li> <li>- Eksternt personale skal underskrive avtale som blant annet dekker taushetserklæring</li> <li>- Alle medarbeidere skal være observante på ukjente personer som ferdes i områder hvor det behandles helse- og personopplysninger</li> <li>- Alle medarbeidere skal rapportere avvik og melde fra om hendelser som kan ha en uheldig virkning på informasjonssikkerheten</li> </ul>
4.	<p><b>Informere de ansatte om reglene for informasjonssikkerhet</b></p> <p>Reglene kan for eksempel gjøres kjent gjennom:</p> <ul style="list-style-type: none"> <li>- Ansettelseskontrakt</li> <li>- Personelhåndbok</li> <li>- Styringssystem for informasjonssikkerhet</li> </ul> <p>For å skape forpliktelse og trygghet for at reglene er forstått anbefales det å utarbeide en avtale mellom virksomheten og den enkelte medarbeider (for eksempel ansettelseskontrakt eller databrukeravtale).</p> <p>Se også Faktaark 9 - Opplæring av ledere og medarbeidere.</p>
5.	<p><b>Kontroll og oppfølging</b></p> <p>For kontroll og oppfølging av daglige retningslinjer for informasjonssikkerhet vises det til Faktaark 2 - Styringssystem for informasjonssikkerhet</p>

## Eksempel

Eksempler på regler for bruk av informasjonsteknologi:

- a) Privat bruk av informasjonssystemet skal godkjennes
- b) Bruk av informasjonssystemet fra hjemmekontor eller på reise skal godkjennes
- c) Flytting/kopiering av helse- og personopplysninger (over på minnepinne, CD mv.) skal godkjennes
- d) Alle data skal sikkerhetskopieres
- e) Utskrifter med helse- og personopplysninger skal oppbevares i låsbart skap og makuleres etter bruk
- f) Elektronisk forsendelse av helse- og personopplysninger (e-post, meldingsutveksling mv.) skal krypteres
- g) Ved fravær fra arbeidsplass og ved arbeidstidens slutt skal bruker logge ut av alle systemer
- h) Alle brukere skal ha egen brukernavn og passord til alle systemer
- i) Oppbevaring, bruk og sikring av passord/PIN-kode skal være iht. fastlagte prosedyrer
- j) Brukernavn og passord skal ikke oppgis på telefon eller e-post
- k) Forespørsler om pasient via e-post skal ikke besvares
- l) Det er ikke tillatt å søke etter informasjon man ikke har behov for eller ikke er autorisert for
- m) Kun jobberelatert informasjon fra Internett kan lastes ned
- n) Programvare skal ikke installeres uten godkjenning
- o) E-post og vedlegg til e-post fra mistenkelig ukjent avsender skal ikke åpnes
- p) Nødprosedyrer skal etableres
- q) Feilsituasjoner skal håndteres iht. fastlagte prosedyrer
- r) Avvik skal rapporteres i avvikssystemet
- s) Virksomheten kan ha innsynsrett i arbeidstakers e-postkasse som arbeidsgiver har stilt til disposisjon til bruk i arbeidet. Tilsvarende har arbeidsgiver adgang til gjennomføring av og innsyn i arbeidstakers personlige område i virksomhetens datanettverk og i andre elektroniske kommunikasjonsmedier eller elektronisk utstyr som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet