

 <p>Norm for informasjonssikkerhet www.normen.no</p>	Utgitt med støtte av: 
<h1>Ansvar og organisering</h1>	<b>Støttedokument</b> <b>Faktaark nr 1</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 checked="" type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
<b>Ansvar</b>	Virksomhetens leder skal påse at informasjonshandlingen og informasjonssikkerheten organiseres slik at det er tydelig hvem som har ansvar for de ulike deler av informasjonshandlingen. Ansvar for informasjonssikkerhet innebærer både et overordnet ansvar for at virksomheten har tilfredsstillende og dekkende informasjonssikkerhet iht helseregisterloven, og et ansvar for at ledere, medarbeidere, innleid personell og leverandører følger de spesifikke krav og plikter som gjelder i virksomheten. Databehandler har et selvstendig ansvar for at Normen følges om dette er regulert i avtale med virksomheten eller Norsk Helsenett.		
<b>Gjennomføring</b>	Ansvar og organisering skal dokumenteres før behandling av helse- og personopplysninger begynner.		
<b>Formål</b>	Beskrive hvordan arbeidet med informasjonssikkerhet organiseres slik at det kommer frem hvem som er ansvarlig på ulike nivåer, og hva de er ansvarlig for.		
<b>Omfang</b>	Enhver virksomhet i helsesektoren og alt arbeid med informasjonssikkerhet som planlegging, styring, gjennomføring og kontroll i virksomheten samt utveksling av helse- og personopplysninger mellom virksomheter.		
<b>Hjemmel</b>	<ul style="list-style-type: none"> <li>• Personopplysningsforskriften § 2-3</li> <li>• Helseforskningsloven § 6</li> </ul>		
<b>Referanser</b>	<ul style="list-style-type: none"> <li>• Norm for informasjonssikkerhet, kap. 3.1 Ansvar</li> <li>• Veileder i personvern og informasjonssikkerhet for helse- og sosialtjenester i kommuner</li> <li>• Veileder for fjernaksess for vedlikehold og oppdateringer fra leverandør til helsevirksomhet</li> <li>• Personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren</li> </ul>		

## Handling/Utførelse

Nr.	Aktivitet/Beskrivelse
1	<p><b>Ansvar for informasjonssikkerhet i store virksomheter (f.eks. sykehus, kommuner mv.)</b></p> <p><b>Styret</b> Styret har det overordnede ansvar for informasjonssikkerheten i virksomheten og skal påse at nødvendige prosedyrer/tiltak er iverksatt for å ivareta denne.</p> <p><b>Virksomhetsleder/adm.dir/rådmann</b></p> <ul style="list-style-type: none"> <li>- Definere mål og strategi for informasjonssikkerhet</li> <li>- Beskrive ansvar og myndighetsforhold (se vedlagt eksempel med hvilke sikkerhetsfunksjoner/-roller som skal finnes i organisasjonen)</li> <li>- Spesifisere hvilke behandlinger helse- og personopplysninger skal ha</li> <li>- Melde og evt søke konsesjon for behandlinger til Datatilsynet</li> <li>- Følge opp og kontrollere informasjonssikkerheten</li> </ul> <p><b>Linjeleder/avdelingsjef</b></p> <ul style="list-style-type: none"> <li>- Videreføre virksomhetsleders ansvar i egen avdeling</li> </ul>

Nr.	Aktivitet/Beskrivelse
	<ul style="list-style-type: none"> <li>- Følge opp og kontrollere informasjonssikkerheten</li> <li>- Prioritere tiltak</li> <li>- Følge opp avtaler om tilgang på tvers av virksomhetsgrenser</li> <li>- Kontroll av tilgang på tvers</li> </ul> <p><b>IKT-ansvarlig</b></p> <ul style="list-style-type: none"> <li>- Sørge for at informasjonssystemet driftes og sikres iht fastsatte krav</li> <li>- Etablere beredskapsløsning</li> <li>- Vurdere eventuell løsning for fjernaksess opp mot veileder for fjernaksess</li> <li>- Følge opp leverandører og databehandler</li> </ul> <p><b>Den enkelte medarbeider</b></p> <ul style="list-style-type: none"> <li>- Følge virksomhetens sikkerhetsbestemmelser</li> </ul>
2	<p><b>Ansvar for informasjonssikkerhet i mindre virksomheter (f.eks. rehabilitering- og opptreningsvirksomheter)</b></p> <p><b>Virksomhetsleder</b></p> <ul style="list-style-type: none"> <li>- Definere mål og strategi for informasjonssikkerhet</li> <li>- Beskrive ansvar og myndighetsforhold (se vedlagt eksempel med hvilke sikkerhetsfunksjoner/-roller som finnes i organisasjonen)</li> <li>- Spesifisere hvilke behandlinger helse- og personopplysninger skal ha</li> <li>- Melde og evt søke konsesjon for behandlinger til Datatilsynet</li> <li>- Følge opp og kontrollere informasjonssikkerheten</li> <li>- Prioritere tiltak</li> </ul> <p><b>Linjeleder/avdelingssjef</b></p> <ul style="list-style-type: none"> <li>- Videreføre virksomhetsleders ansvar</li> <li>- Følge opp avtaler tilgang på tvers av virksomhetsgrenser</li> <li>- Kontroll av tilgang på tvers</li> </ul> <p><b>IKT-ansvarlig</b></p> <ul style="list-style-type: none"> <li>- Sørge for at informasjonssystemet driftes og sikres iht fastsatte krav</li> <li>- Vurdere eventuell løsning for fjernaksess opp mot veileder for fjernaksess</li> <li>- Følge opp leverandører og databehandler</li> </ul> <p><b>Den enkelte medarbeider</b></p> <ul style="list-style-type: none"> <li>- Følge virksomhetens sikkerhetsbestemmelser</li> </ul>
3	<p><b>Ansvar for informasjonssikkerhet i små virksomheter (f.eks. legekantor, tannlekantor, fysioterapinstitutt, psykologfellesskap, bedriftshelsetjeneste, mv.)</b></p> <p><b>Daglig leder/virksomhetenes leder</b></p> <ul style="list-style-type: none"> <li>- Definere mål og strategi for informasjonssikkerhet</li> <li>- Beskrive ansvar og myndighetsforhold (benytt vedlagte eksempel til å definere ansvarsområder)</li> <li>- Spesifisere hvilke behandlinger helse- og personopplysninger skal ha</li> <li>- Melde og evt søke konsesjon for behandlinger til Datatilsynet</li> <li>- Vurdere eventuell løsning for fjernaksess opp mot veileder for fjernaksess</li> <li>- Følge opp og kontrollere informasjonssikkerheten (inklusive databehandler)</li> <li>- Følge opp avtaler om tilgang på tvers av virksomhetsgrenser</li> <li>- Kontroll av tilgang på tvers</li> <li>- Prioritere tiltak</li> </ul>

## **Eksempel**

Se neste side. Eksempelet er hentet fra et helseforetak og gir en oversikt over mulige roller og ansvarsområder. Oversikten er ment å brukes som en sjekkliste slik at aktuelle områder blir vurdert og ansvaret plassert. Matrisen må tilpasses lokale forhold og for eksempel utvides med: forskningsansvarlig, forsker og prosjektleder.

Et tilsvarende eksempel, spesielt myntet på kommuner, finnes i "Veileder i personvern og informasjonssikkerhet for helse- og sosialtjenester i kommuner"

Eksempel på sikkerhetsansvar, -roller og -oppgaver internt i virksomheten

## Matrisen må tilpasses lokale forhold

<b>Funksjon:</b>	<b>Daglig leder</b>	<b>Avdelingsleder</b>	<b>Bruker</b>	<b>IKT-ansvarlig</b>	<b>IKT-sikkerhetsleder</b>	<b>Systemeier</b>
<b>Ansvar</b>	<ul style="list-style-type: none"> <li>- Sørge for at det er etablert et Styringssystem for IKT-sikkerhet og at dette vedlikeholdes.</li> <li>- Sørge for at informasjonssikkerheten er tilfredsstillende.</li> <li>- Bestemme formålet med behandlingen av personopplysninger</li> <li>- Bestemme hvilke hjelpemidler som skal brukes</li> </ul>	<ul style="list-style-type: none"> <li>- Sørge for opplæring av ansatte</li> <li>- Beredskap</li> <li>- Tildeling, vedlikehold og inndragning av roller/ tilgang</li> <li>- Rapportere avvik i samsvar med foretakets prosedyrer for dette</li> <li>- Følge opp forskningsprosjekt</li> </ul>	<ul style="list-style-type: none"> <li>- Gjøre seg kjent med og følge lover, regler og prosedyrer</li> <li>- Melde avvik</li> </ul>	<ul style="list-style-type: none"> <li>- Sørge for at informasjonssystemet er tilgjengelig</li> <li>- Sørge for at informasjonssystemet oppfyller lovbestemte og andre krav</li> <li>- Sørge for at informasjonssystemet fungerer som besluttet</li> <li>- Etablere ansvarskart for informasjonssystemet</li> </ul>	<ul style="list-style-type: none"> <li>- Overvåke at informasjonssystemet benyttes i samsvar med bestemmelser og prosedyrer</li> <li>- Rapportere til databehandlingsansvarlig</li> </ul>	<ul style="list-style-type: none"> <li>- Sørge for at sitt informasjonssystem er tilgjengelig</li> <li>- Sørge for at sitt informasjonssystem oppfyller lovbestemte og andre krav</li> <li>- Sørge for at sitt informasjonssystem fungerer som besluttet</li> <li>- Definere tilgangsroller</li> <li>- Rapportere til IKT-ansvarlig</li> </ul>
<b>Rolle</b>	<i>Databehandlingsansvarlig</i>	<i>Leder med personalansvar</i>	<i>Systembruker</i>	<i>Bestiller</i>	<i>Sikkerhetsansvarlig</i>	<i>Systemeier for et system</i>
<b>Oppgaver</b>	<ul style="list-style-type: none"> <li>- Vedta, implementere, vedlikeholde og følge opp bruken av Styringssystem for IKT-sikkerhet</li> <li>- Melde og evt søke konsesjon for behandlinger til Datatilsynet</li> </ul>	<ul style="list-style-type: none"> <li>- Sørge for at det gis opplæring i nødvendige systemer og i sikkerhet</li> <li>- Lage og teste beredskapsprosedyrer for systemsvikt</li> <li>- Tildele den enkelte medarbeider korrekt rolle og bestille tilgang til nettverk og system</li> <li>- Vedlikeholde medarbeidernes tilgangsnivå</li> <li>- Inndra tilgang ved opphør av arbeidsforhold</li> <li>- Sørge for at forskningsprosjekt blir meldt til NSD/Datatilsynet</li> <li>- Følge opp at forskningsprosjekt følger meldt plan eller tildelt konsesjon</li> <li>- Håndtere sikkerhetsavvik</li> <li>- Kontroll av tilgang på tvers</li> </ul>	<ul style="list-style-type: none"> <li>- Lese og følge gjeldende regler</li> <li>- Gjøre seg kjent med Internkontrollsystem for personopplysninger</li> </ul>	<ul style="list-style-type: none"> <li>- Utarbeide og vedlikeholde prosedyrer rundt egen funksjon</li> <li>- Utarbeide og inngå serviceavtale om drift og vedlikehold av informasjonssystemet</li> <li>- Utarbeide beredskapsplan</li> <li>- Gjennomføre endringsledelse ved endringer av informasjonssystemet</li> <li>- Sørge for risikovurderinger og overvåke risiko</li> <li>- Vurdere eventuell løsning for fjernaksess opp mot veileder for fjernaksess</li> <li>- Følge opp partnere, leverandør og databehandlere i forhold til sikkerhet</li> <li>- Håndtere meldte avvik</li> <li>- Rådgiving</li> <li>- Sørge for at det blir utpekt systemeier for det enkelte system og holde oversikt over disse.</li> </ul>	<ul style="list-style-type: none"> <li>- Utarbeide og vedlikeholde prosedyrer rundt egen funksjon</li> <li>- Utforming av styrende, utførende og kontrollerende dokument i foretakets Internkontrollsystem/ sikkerhetskåndbok</li> <li>- Forberede ledergruppens årlige gjennomgang</li> <li>- Følge opp iverksetning av tiltak som er besluttet etter gjennomgang</li> <li>- Samordne og gjennomføre sikkerhetsrevisjoner</li> <li>- Vurdere rapporterte avvik</li> <li>- Forestå risikovurderinger</li> <li>- Godkjenne dokument til foretakets internkontrollsystem/ sikkerhetskåndbok</li> <li>- Erverve og vedlikeholde kunnskap om trusler, sårbarhet, sikkerhetstiltak og –teknikker, sikkerhetskrav</li> <li>- Opplæring</li> <li>- Rådgiving</li> </ul>	<ul style="list-style-type: none"> <li>- Utarbeide og vedlikeholde prosedyrer rundt egen funksjon</li> <li>- Bistå IKT-ansvarlig i å utarbeide vedlegg til serviceavtale</li> <li>- Bistå IKT-ansvarlig i å utarbeide avtaler om endringer av sitt systems konfigurasjon</li> <li>- Definere tilgangsroller for sitt system og gjøre disse kjent</li> <li>- Sørge for risikovurderinger og overvåke risiko</li> <li>- Følge opp partnere, leverandør og databehandlere i forhold til sikkerhet</li> <li>- Håndtere meldte avvik</li> <li>- Oppfølging tilgang på tvers av virksomhetsgrenser</li> </ul>