

 <p>Norm for informasjonssikkerhet www.normen.no</p>	Utgitt med støtte av:  Helsedirektoratet
<h2>Oversikt over anbefalte prosedyrer i styringssystemet for informasjonssikkerhet</h2>	Støttedokument Faktaark nr 3 Versjon: 2.1 Dato: 15.12.2010

Målgruppe Dette faktaarket er spesielt relevant for:	<input type="checkbox"/> Leverandør <input type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input checked="" 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 type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
Ansvar	Virksomhetens ledelse og forskningsansvarlig er ansvarlig for at virksomheten har de nødvendige prosedyrer i styringssystem for informasjonssikkerhet.		
Gjennomføring	Prosedyrer i styringssystem for informasjonssikkerhet skal etableres før behandling av helse- og personopplysninger.		
Formål	Gi databehandlingsansvarlig og forskningsansvarlig en oversikt over de mest sentrale prosedyrene i styringssystemet for informasjonssikkerhet.		
Omfang	Omfanget av prosedyrene skal tilpasses virksomhetens art, aktiviteter og størrelse.		
Hjemmel	<ul style="list-style-type: none"> • Personopplysningsforskriften kap. 2. • Helseforsningsloven § 6 		
Referanser	Norm for informasjonssikkerhet, kap. 3.2.		

Oversikt over anbefalte prosedyrer i styringssystemet dekker deler som kan inngå i et styringssystem for informasjonssikkerhet. For forslag til oppbygging av styringssystem for informasjonssikkerhet, se Faktaark 2 - Styringssystem for informasjonssikkerhet.

Oversikten under har en tredeling: styrende, gjennomførende og kontrollerende del. Dette faktaarket har spesielt fokus på den gjennomførende delen.

1. Styrende del

Anbefalte elementer i styrende del:
<ul style="list-style-type: none"> - Akseptkriterier for risiko - Beskrivelse av databehandlingsansvaret - Beskrivelse av sikkerhetsorganisasjon - Fastsettelse av hjemmelsgrunnlaget for behandlingene - Formålet med behandlingene - Oversikt over behandlinger - Sikkerhetsmål og –strategi - Systemoversikt og klassifisering av systemer - IKT-sikkerhetsinstruks

2. Gjennomførende del

Prosedyrer i gjennomførende del:
Virksomheten skal utarbeide prosedyrer for:
<ul style="list-style-type: none"> - Gjennomføring av risikovurderinger - Bestilling, endring og sletting av brukerkontoer - Håndtering av utskrifter med helse- og personopplysninger - Oppbevaring av dokumenter med helse- og personopplysninger - Opplæring i informasjonssikkerhet - Pasienters innsyn i helse- og personopplysninger

Prosedyrer i gjennomførende del:

- Plikt til å gi informasjon til den registrerte om personvernrettigheter
- Bruk av Norsk Helsenett (helsenettet)
- Hindre ødeleggende dataprogram
- Fysisk sikring av rom og områder
- Hendelsesregistrering
- Håndtering av passord
- Sikkerhetskopi (backup)
- Retting av helse- og personopplysninger
- Innhenting av informert samtykke
- Ivaretagelse av reservasjonsretten
- Konfigurasjonskontroll
- Makulering av dokumenter med helse- og personopplysninger
- Meldeplikt eller søknad om konsesjon (til Datatilsynet)
- Oppretting og vedlikehold av autorisasjonsregister
- Sletting av helse- og personopplysninger
- Taushets- og brukererklæring for ansatte
- Utlevering av helse- og personopplysninger til andre

Virksomheten bør utarbeide prosedyrer for:

- Bruk av databehandler
- Bruk av bærbart datautstyr
- Forskning på helse- og personopplysninger
- Krav til IKT-leverandører ifm service og vedlikehold
- Meldingskommunikasjon med helse- og personopplysninger
- Nødprosedyrer ved manuell drift
- Håndtering av flyttbare datalagringsmedier
- Bruk av trådløs teknologi
- Bruk datanettverk
- Sikkerhet i nettverks- og tilgangssoner
- Tilknytning av leverandører for fjernaksess
- Taushetserklæring og autorisasjon for fjernaksess for interne IKT-konsulenter
- Taushetserklæring og skjema for autorisasjon av servicemedarbeider til fjernadgang
- Tilgangsstyring og kontroll av tilgang på tvers

3. Kontrollerende del**Anbefalte prosedyrer for oppfølging og kontroll:**

- Risikovurdering
- Avviksbehandling
- Ledelsens gjennomgang (gjennomføres minimum årlig)
- Sikkerhetsrevisjon (gjennomføres minimum årlig)