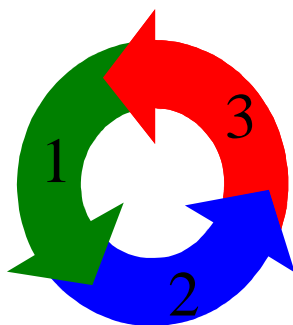


		Utgitt med støtte av: 
Norm for informasjonssikkerhet <a href="http://www.normen.no">www.normen.no</a>		
<h1>Styringssystem for informasjonssikkerhet</h1>		<b>Støttedokument</b> <b>Faktaark nr 2</b> Versjon: 2.1 Dato: 15.12.2010

<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 type="checkbox"/> Medarbeider/ansatt <input type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
<b>Ansvar</b>	Virksomhetens ledelse er ansvarlig for å etablere og innføre et styringssystem for informasjonssikkerhet.		
<b>Gjennomføring</b>	Styringssystem for informasjonssikkerhet skal etableres ved behandling av helse- og personopplysninger.		
<b>Formål</b>	<ul style="list-style-type: none"> <li>Dokumentere en oversikt over konkrete og praktiske aktiviteter som databehandlingsansvarlige skal gjennomføre for å styre virksomheten når det gjelder informasjonssikkerhet</li> <li>Danne grunnlag for etablering av nødvendige sikkerhetstiltak i den enkelte virksomhet ift relevante trusler som kan påvirke behandling av helse- og personopplysninger, slik at bruk og behandling av helse- og personopplysninger skjer iht krav i personopplysningsforskriften kapittel 2</li> </ul>		
<b>Omfang</b>	Alle virksomheter i helsesektoren skal etablere styringssystem for informasjonssikkerhet. Omfang av styringssystemet skal være tilpasset virksomhetens størrelse og omfanget av behandling av helse- og personopplysninger.		
<b>Hjemmel</b>	<ul style="list-style-type: none"> <li>Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer, Desember 2000, Datatilsynet, Del I, Innledning, avsnitt 3</li> </ul>		
<b>Referanser</b>	<ul style="list-style-type: none"> <li>NS ISO 27002 Informasjonsteknologi - Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet</li> <li>Norm for informasjonssikkerhet, kap 4.1 Styringssystem for informasjonssikkerhet</li> </ul>		



Styringssystem for informasjonssikkerhet skal sikre at personvernet og sikkerhetsarbeidet blir en kontinuerlig prosess og ivaretatt på en systematisk og dokumentert måte. Omfanget av styringssystemet skal være ift virksomhetens størrelse og behandling av helse- og personopplysninger. Se eksempel under for oppbygging av styringssystem for informasjonssikkerhet.

## Eksempel på oppbygging av styringssystem for informasjonssikkerhet

### 1. Styrende del

- Beskrivelse av ledelse og organisering av informasjonssikkerhet
- Beskrivelse av og oversikt over formålet med behandlingene
- Fastsettelse av sikkerhetsmål og -strategi
- Fastsettelse av nivå for akseptabel risiko

### 2. Gjennomførende del

- Prosedyrer
- Dokumentasjon av sikkerhetstiltak
- Opplæring

3. Kontrollerende del
  - a) Risikovurdering
  - b) Sikkerhetsrevisjon
  - c) Avvikshåndtering
  - d) Ledelsens gjennomgang

Se også Faktaark 3 - Oversikt over anbefalte prosedyrer i styringssystemet.

### Handling/Utførelse

Nr.	Aktivitet/Beskrivelse
1	<p><b>Organisering og styring av informasjonssikkerhet</b></p> <ul style="list-style-type: none"> <li>- Ansvarsforhold beskrives slik at det er tydelig hvem som er ansvarlig på ulike nivåer og hva de er ansvarlig for (hva dette ansvaret innebærer)</li> <li>- Formål med behandling av helse- og personopplysninger beskrives slik at det er tydelig hva helse- og personopplysningene benyttes til</li> <li>- Mål for informasjonssikkerhet defineres. På grunnlag av målene skal det fastsettes et nivå for akseptabel risiko (akseptkriterier) slik at det er mulig å kontrollere om sikkerhetsmålene nåes</li> <li>- Sikkerhetsstrategi for å nå sikkerhetsmålene (og nivå for akseptabel risiko) utarbeides. Strategien skal vise valg og prioritering av sikkerhetstiltak</li> </ul>
2	<p><b>Gjennomføring</b></p> <ul style="list-style-type: none"> <li>- Det skal føres oversikt over helse- og personopplysninger som behandles i virksomheten. I oversikten skal hjemmelsgrunnlaget for behandlingen angis og tidspunkt for når melding evt. konsesjonssøknad er sendt Datatilsynet</li> <li>- Oversikt over partnere og leverandører skal dokumenteres. Virksomheten skal etablere klare ansvarsforhold mellom partnere og leverandører som beskrives i en særskilt avtale</li> <li>- Konfigurasjonskart og beskrivelse av den IT-tekniske løsningen skal utarbeides. Løsningen skal baseres på valgt sikkerhetsstrategi og risikovurderinger</li> <li>- Prosedyrer for informasjonsbehandlingen skal dokumenteres og innføres</li> <li>- Risikovurderinger skal gjennomføres for å kartlegge risikoområder og klarlegge sannsynligheten for og konsekvens av uønskede hendelser (sikkerhetsbrudd). Hver enhet og hvert nivå ved respektive ledelse skal gjennomføre risikovurderinger periodisk og etter fastsatte maler og retningslinjer. Risikovurdering skal som minimum gjennomføres før:           <ul style="list-style-type: none"> <li>o etablering av nye informasjonssystemer eller registre som inneholder helse- og personopplysninger</li> <li>o organisatoriske endringer som kan påvirke informasjonsbehandlingen</li> <li>o større konfigurasjons- og systemendringer</li> </ul> </li> </ul>
3	<p><b>Kontroll og oppfølging</b></p> <ul style="list-style-type: none"> <li>- Ledelsen skal utarbeide og vedta en plan for risikovurderinger</li> <li>- Ledelsen skal foreta kontroll av risikovurderingene og påse at resultatet av risikovurderingene er i henhold til fastlagte akseptkriterier</li> <li>- Sikkerhetsrevisjoner skal gjennomføres jevnlig og minimum årlig. Ledelsen skal utarbeide og vedta en plan for sikkerhetsrevisjoner i virksomheten</li> <li>- Avvikshåndtering iverksettes ved sikkerhetsbrudd og/eller når oppgaver utføres i strid med gjeldende prosedyrer eller "vanlig praksis". Virksomheten skal ha en egen prosedyre for håndtering av avvik</li> <li>- Ledelsens gjennomgang skal gjennomføres iht utarbeidet møteplan. Formålet med ledelsens gjennomgang er å avdekke om sikkerheten ivaretas iht mål, strategier og prosedyrer og beslutte handlingsplaner for det videre sikkerhetsarbeidet. Ledelsens gjennomgang skal gjennomføres minimum årlig og i sammenheng med årlig økonomi- eller virksomhetsplanlegging</li> </ul>