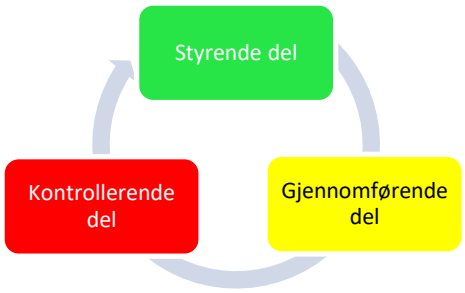
NORMEN **Norm for informasjonssikkerhet** **www.normen.no**	Utgitt med støtte av: Direktoratet for e-helse
Styringssystem for informasjonssikkerhet og personvern	**Støttedokument** **Faktaark nr 2** Versjon: 3.2 Dato: 24.10.2019

Formål	• Sikre at arbeidet med informasjonssikkerhet og personvern ivaretas på en systematisk måte • Dokumentere ledelsens krav til informasjonssikkerhet og personvern, rutiner som ansatte og medarbeidere skal følge for å nå virksomhetens krav og kontrollmekanismer som skal benyttes for å kontrollere at kravene blir oppnådd • Være grunnlag for at nødvendige sikkerhetstiltak etableres i virksomheten ift relevante trusler som kan påvirke behandlingen av helse- og personopplysninger • Gi dataansvarlig en oversikt over relevante dokumenter i styringssystemet		
Ansvar	Virksomhetens øverste ledelse skal sørge for å etablere og innføre et styringssystem for informasjonssikkerhet.		
Gjennomføring	Styringssystem for informasjonssikkerhet og personvern skal etableres ved behandling av helse- og personopplysninger.		
Omfang	Alle virksomheter i helse- og omsorgstjenesten skal etablere styringssystem for informasjonssikkerhet og personvern. Omfanget av styringssystemet skal tilpasses virksomhetens størrelse og omfanget av behandlingen av helse- og personopplysninger.		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Virksomhetens leder/ledelse ☐ Forskningsansvarlig ☐ Prosjektleder forskning ☒ Sikkerhetsleder	☐ Ansatt / medarbeider ☐ Forsker ☒ Personvernombud	☐ IKT-ansvarlig ☒ Databehandler ☐ Leverandør
Hjemmel	• Personvernforordningen artikkel 24 og 32 • Pasientjournalloven §§ 22 og 23 • eForvaltningsforskriften § 15		
Referanser	• Norm for informasjonssikkerhet, kap 2 Styringssystem • Veileder for små helsevirksomheter (lenke) • Difis veiledningsmateriell: https://internkontroll-infosikkerhet.difi.no/ • ISO/IEC 27001:2013 Informasjonsteknologi - Sikringsteknikk – Styringssystem for informasjonssikkerhet - Krav		

Det utarbeides en egen veileder for små helsevirksomheter med forslag til innhold i et styringssystem.

Styringssystem for informasjonssikkerhet og personvern (internkontroll) skal sikre at arbeidet med personvern og informasjonssikkerhet blir en kontinuerlig prosess og ivaretatt på en systematisk og dokumentert måte. Styringssystemet skal tilpasses virksomhetens størrelse, egenart og aktiviteter og behandlingene av helse- og personopplysningenes art, omfang, formål og sammenhengen den utføres i. Det anbefales å innarbeide styringssystemet i virksomhetens øvrige internkontroll.

Eksempelet nedenfor består av en styrende, gjennomførende og kontrollerende del.



Den styrende delen inneholder ledelsens krav til personvern og informasjonssikkerhet og beskriver de overordnede føringene som gjelder i virksomheten. Videre beskrives sikkerhetsorganisasjonen med hvilke roller som er ansvarlig for oppgavene på ulike nivåer. Som utgangspunkt for arbeidet med personvern og informasjonssikkerhet utarbeides og vedlikeholdes det en oversikt med hvilke behandlinger av helse- og personopplysninger virksomheten utfører.

Den gjennomførende delen inneholder alle detaljerte regler og krav for personvern og informasjonssikkerhet som skal følges i virksomheten og skal dekke kravene i den styrende del. Reglene og kravene gjelder både ledelsen, den enkelte ansatte og medarbeider og ansvarlige for informasjonsteknologi.

Den kontrollerende delen inneholder kontrollmekanismene som skal benyttes for å kontrollere at kravene blir oppnådd og at Rutinene følges.

Eksempel på innhold i styringssystem informasjonssikkerhet:

1. Styrende del:

- Overordnede føringer for bruk av informasjonsteknologi
- Beskrivelse av roller og ansvar i arbeidet med informasjonssikkerhet og personvern
- Oversikt over behandlinger av helse- og personopplysninger (protokoll, se faktaark 35)
- Offentlige virksomheter må beskrive sikkerhetsmål og etablere strategi
- Nivå for akseptabel risiko
- Systemoversikt og klassifisering av systemer
- IKT-sikkerhetsinstruks
- Rutine for opplæring av ansatte
- Rutine for plan for-, gjennomføring av-, og oppfølging av resultater fra risikovurdering (Se faktaark 7)

2. Gjennomførende del:

Virksomheten skal utarbeide:

- Oversikt over databehandlere og leverandører med avtaler
- Rutine for gjennomføring av risikovurdering (se faktaark 7)
- Konfigurasjonskart over informasjonssystemene og teknisk beskrivelse av konfigurasjonen
- Rutine for konfigurasjonskontroll
- Beskrivelse av løsning for å hindre ødeleggende dataprogram
- Rutine for oppretting og vedlikehold av autorisasjonsregister
- Rutine for hendelsesregistrering
- Regler for håndtering av passord
- Rutine for sikkerhetskopiering (backup)
- Bruk av Norsk Helsenett (helsenettet)
- Regler for fysisk sikring av lokaler og områder

- Rutine for innhenting av informert samtykke
- Rutine for den registrertes innsyn i helse- og personopplysninger
- Rutine for ivaretakelse av reservasjonsretten
- Rutine for å gi informasjon til den registrerte om personvernrettigheter
- Rutine for retting av helse- og personopplysninger

2. Gjennomførende del:

- Rutine for sletting av helse- og personopplysninger

- Rutine for bestilling, endring og sletting av brukerkontoer
- Rutine for håndtering av utskrifter med helse- og personopplysninger
- Rutine for oppbevaring av dokumenter med helse- og personopplysninger
- Rutine for makulering av dokumenter med helse- og personopplysninger
- Rutine for opplæring i informasjonssikkerhet
- Rutiner for bruk av informasjonssystemer
- Taushetserklæring for ansatte ved tiltredelse
- Rutine og skjema for taushets- og brukererklæring for andre som skal ha tilgang til helse- og personopplysninger
- Rutine for utlevering av helse- og personopplysninger til andre

Virksomheten bør utarbeide (ut fra behov):

- Bruk av databehandler
- Rutine for forskning på helse- og personopplysninger
- Rutine for tilgangsstyring
- Rutine for tilgang til helseopplysninger mellom virksomheter
- Rutine for kontroll av tilgang til helseopplysninger mellom virksomheter
- Avtale om samarbeid om behandlingsrettede helseregistre
- Rutine for utlevering av helseopplysninger til kvalitetssikring og læring

- **Nødrutine** for manuell drift
- Rutine for håndtering av flyttbare datalagringsmedier
- Rutine for bruk datanettverk
- Rutine for bruk av trådløs teknologi
- Regler for sikkerhet i nettverks- og tilgangssoner
- Rutine for bruk av mobilt utstyr
- Krav til autentisering ved tilgang til helse- og personopplysninger via mobilt utstyr
- Rutiner for bruk av standard meldinger for kommunikasjon av helse- og personopplysninger

- Rutine for tilknytning av leverandør for fjernaksess
- Krav til IKT-leverandør ved service og vedlikehold
- Taushetserklæring og autorisasjon for fjernaksess for intern IKT-konsulent
- Taushetserklæring og skjema for autorisasjon av servicemedarbeider til fjernaksess

3. Kontrollerende del:

- Rutine for avviksbehandling (se faktaark 8)
- Rutine for ledelsens gjennomgang (gjennomføres minimum en gang i året) (Se Normen kapittel 2.5)
- Rutine for regelmessig gjennomføring av sikkerhetsrevisjoner (Se faktaark 6)
- Rutine for oppfølging av resultater av risikovurdering