Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Ansvar og organisering

Støttedokument
Faktaark nr 1
Versjon: 3.1
Dato: 18.09.2018

Formål	Beskrive organisering av arbeidet med informasjonssikkerhet slik at det tydelig kommer frem hvem som er ansvarlig på ulike nivåer, og hva de er ansvarlig for.		
Ansvar	Dataansvarlig skal påse at behandlingen av helse- og personopplysninger og informasjonssikkerheten organiseres slik at det er tydelig hvem som har ansvar for de ulike deler av behandlingen. Ansvaret for informasjonssikkerhet innebærer både et overordnet ansvar for at virksomheten har tilfredsstillende og dekkende informasjonssikkerhet iht Normen, og et ansvar for at ledere på alle nivåer, ansatte/medarbeidere, innleid personell og leverandører følger de spesifikke krav og plikter som gjelder i virksomheten. Databehandler har et selvstendig ansvar for at Normen følges slik det er regulert i avtale med virksomheten eller Norsk Helsenett.		
Gjennomføring	Ansvar og organisering skal dokumenteres før behandling av helse- og personopplysninger begynner.		
Omfang	Enhver virksomhet i helse- og omsorgstjenesten skal dokumentere ansvar og organisering av arbeidet med informasjonssikkerhet.		
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 • Helseforskningsloven § 6 • Pasientjournalloven §§ 22 og 23		
Referanser	• Norm for informasjonssikkerhet, kap. 2		

Merknad 18.09.2018: Utdaterte hjemler og referanser er fjernet, men dokumentet kan inneholde tekst som er foreldet ut fra siste versjon av Normen, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

Dataansvarlig er ansvarlig for informasjonssikkerheten i virksomheten og skal påse at nødvendige tiltak er iverksatt for å ivareta denne.

Nr.	Ansvar i virksomheten
1	**Ansvar for informasjonssikkerhet i <u>store virksomheter</u> (f.eks. sykehus, kommune mv.)** **Virksomhetens leder**[1] - Fastsette mål og strategi for informasjonssikkerhet - Fastsette nivå for akseptabel risiko - Beskrive ansvar og myndighetsforhold (se vedlagt eksempel med hvilke sikkerhetsfunksjoner/-roller som skal finnes i organisasjonen) - Fastsette hvilke behandlinger av helse- og personopplysninger som skal utføres i virksomheten - Melde og eventuelt søke konsesjon for behandlinger til Datatilsynet - Følge opp og kontrollere informasjonssikkerheten **Leder**

[1] I en kommune er ordfører formelt ansvarlig, mens rådmann vil være utførende ansvarlig

Nr.	Ansvar i virksomheten
	- Følge opp virksomhetsleders ansvar i egen avdeling - Følge opp og kontrollere informasjonssikkerheten - Prioritere og gjennomføre tiltak - Etablere og følge opp avtaler om tilgang på tvers - Kontrollere tilgang på tvers **IKT-ansvarlig** - Sørge for at informasjonssystemet driftes og sikres iht fastsatte krav - Etablere beredskapsløsning - Vurdere eventuell løsning for fjernaksess opp mot veileder for fjernaksess - Følge opp leverandører og databehandler **Ansatt/medarbeider** - Følge virksomhetens sikkerhetsprosedyrer
2	**Ansvar for informasjonssikkerhet i <u>mindre virksomheter</u> (f.eks. rehabilitering- og opptreningsvirksomheter)** **Virksomhetens leder** - Definere mål og strategi for informasjonssikkerhet - Fastsette nivå for akseptabel risiko - Beskrive ansvar og myndighetsforhold (se vedlagt eksempel med hvilke sikkerhetsfunksjoner/-roller som finnes i organisasjonen) - Fastsette hvilke behandlinger av helse- og personopplysninger som skal utføres i virksomheten - Melde og eventuelt søke konsesjon for behandlinger til Datatilsynet - Følge opp og kontrollere informasjonssikkerheten - Prioritere og gjennomføre tiltak **Leder** - Videreføre virksomhetsleders ansvar - Etablere og følge opp avtaler om tilgang på tvers - Kontrollere tilgang på tvers **IKT-ansvarlig** - Sørge for at informasjonssystemet driftes og sikres iht fastsatte krav - Vurdere eventuell løsning for fjernaksess opp mot veileder for fjernaksess - Følge opp leverandører og databehandler **Ansatt / medarbeider** - Følge virksomhetens sikkerhetsprosedyrer
3	**Ansvar for informasjonssikkerhet i <u>små virksomheter</u> (f.eks. apotek, bedriftshelsetjeneste, fysioterapiinstitutt, legekontor, psykologfellesskap tannlegekontor, mv.)** **Virksomhetens leder** - Definere mål og strategi for informasjonssikkerhet - Fastsette nivå for akseptabel risiko - Beskrive ansvar og myndighetsforhold (benytt vedlagte eksempel til å definere ansvarsområder)

Nr.	Ansvar i virksomheten
	- Fastsette hvilke behandlinger av helse- og personopplysninger som skal utføres i virksomheten - Melde og eventuelt søke konsesjon for behandlinger til Datatilsynet - Vurdere eventuell løsning for fjernaksess opp mot veileder for fjernaksess - Følge opp og kontrollere informasjonssikkerheten (inklusive databehandler) - Etablere og følge opp avtaler om tilgang på tvers - Kontrollere tilgang på tvers - Prioritere tiltak

Eksempler på de neste sidene

Eksemplene er hentet fra helseforetak og gir en oversikt over mulige roller og ansvarsområder. Eksemplene er ment til inspirasjon slik at ansvarsområder blir vurdert og ansvaret plassert. Matrisen må tilpasses lokale forhold og for eksempel utvides med: personvernombud, forskningsansvarlig, forsker og prosjektleder.

	Eksempel 1 på sikkerhetsansvar, -roller og -oppgaver internt i virksomheten **Matrisen må tilpasses lokale forhold** **<Virksomhet>**					
Funksjon:	**Virksomhetens leder**	**Leder**	**Ansatt/Medarbeider**	**IKT-ansvarlig**	**Sikkerhetsleder**	**Systemeier**
Ansvar	- Sørge for at det er etablert et Styringssystem for informasjonssikkerhet og at dette vedlikeholdes - Sørge for at informasjonssikkerheten er tilfredsstillende - Bestemme formålet med behandlingen av personopplysninger - Bestemme hvilke hjelpemidler som skal brukes	- Sørge for opplæring av ansatte - Beredskap - Tildele, vedlikeholde og inndra roller/ tilgang - Rapportere avvik i samsvar med virksomhetens prosedyrer for dette - Følge opp forskningsprosjekt	- Gjøre seg kjent med og følge lover, regler og prosedyrer - Melde avvik	- Sørge for at informasjonssystemet er tilgjengelig - Sørge for at informasjonssystemet oppfyller Normens krav - Sørge for at informasjonssystemet fungerer som besluttet - Etablere ansvarskart for informasjonssystemet	- Overvåke at informasjonssystemet benyttes i samsvar med bestemmelser og prosedyrer - Rapportere til dataansvarlig	- Sørge for at sitt informasjonssystem er tilgjengelig - Sørge for at sitt informasjonssystem oppfyller Normens krav - Sørge for at informasjonssystemet fungerer som besluttet - Definere tilgangsroller - Rapportere til IKT-ansvarlig
Rolle	*Dataansvarlig*	*Leder med personalansvar*	*Systembruker*	*Bestiller*	*Informasjonssikkerhetsleder*	*Systemeier for et system*
Oppgaver	- Vedta, implementere, vedlikeholde og følge opp bruken av styringssystem for informasjonssikkerhet - Gjennomføre ledelsens gjennomgang - Melde og eventuelt søke konsesjon for behandlinger til Datatilsynet	- Sørge for at det gis opplæring i nødvendige systemer og i informasjonssikkerhet - Lage og teste beredskapsprosedyrer for systemsvikt - Sørge for risikovurderinger og overvåke risiko - Tildele den enkelte medarbeider korrekt rolle og bestille tilgang til nettverk og system - Vedlikeholde medarbeidernes tilgangsnivå - Inndra tilgang ved opphør av arbeidsforhold - Sørge for at forskningsprosjekt blir meldt til den regionale etiske komité (REK) - Følge opp at forskningsprosjekt følger meldt plan eller tildelt konsesjon - Behandle avvik - Etablere og følge opp avtaler om tilgang på tvers - Kontrollere tilgang på tvers	- Lese og følge gjeldende regler - Gjøre seg kjent med styringssystem for informasjonssikkerhet	- Utarbeide og vedlikeholde prosedyrer rundt egen funksjon - Utarbeide og inngå serviceavtale om drift og vedlikehold av informasjonssystemet - Utarbeide beredskapsplan - Ivareta konfigurasjonskontroll ved endringer av informasjonssystemet - Sørge for risikovurderinger og overvåke risiko - Vurdere eventuell løsning for fjernaksess opp mot veileder for fjernaksess - Følge opp partnere, leverandør og databehandlere i forhold til informasjonssikkerhet - Håndtere meldte avvik - Rådgiving - Sørge for at det blir utpekt systemeier for det enkelte system og holde oversikt over disse	- Utarbeide og vedlikeholde prosedyrer rundt egen funksjon - Utforming av styrende, utførende og kontrollerende dokument i styringssystemet for informasjonssikkerhet - Forberede ledelsens gjennomgang - Følge opp iverksetting av tiltak som er besluttet gjennomført - Samordne og gjennomføre sikkerhetsrevisjoner - Vurdere rapporterte avvik - Forestå risikovurderinger - Godkjenne dokument til styringssystemet for informasjonssikkerhet - Erverve og vedlikeholde kunnskap om trusler, sårbarhet, sikkerhetstiltak og –teknikker, sikkerhetskrav - Opplæring - Rådgiving	- Utarbeide og vedlikeholde prosedyrer rundt egen funksjon - Bistå IKT-ansvarlig i å utarbeide vedlegg til serviceavtale - Bistå IKT-ansvarlig i å utarbeide avtaler om endringer av sitt systems konfigurasjon - Definere tilgangsroller for sitt system og gjøre disse kjent - Sørge for risikovurderinger og overvåke risiko - Følge opp partnere, leverandør og databehandlere i forhold til informasjonssikkerhet - Håndtere meldte avvik - Følge opp tilgang på tvers

Eksempel 2 på sikkerhetsansvar, -roller og -oppgaver internt i virksomheten

Matrisen må tilpasses lokale forhold
<Virksomhet>

Seksjon	Dok nr.	Versjon	Tittel	Nivå	Side
Organisasjon			**Sikkerhetsansvar, -roller og -oppgaver *internt* i virksomheten**	**1**	**1/1**

Funksjon:	**Daglig leder** *(Dataansvarlig)*	**Avdelingsleder** *(Personalansvar)*	**Bruker (av IKT system)**	**IKT - leder**	**IKT – sikkerhetsleder** *(tilsyns- og rådgiverfunksjon)*	**Systemeier** *(ett eller flere system)*	**Personvernombud**
Ansvar og oppgaver	- Bestemme formålet med behandlingen av personopplysninger - Etablere funksjon for IKT sikkerhet i virksomheten (IKT sikkerhetsleder) - Sørge for at Styringssystem for IKT-sikkerhet er etablert og overholdt i egen virksomhet - Sørge for at informasjonssikkerheten er i samsvar med vedtatt sikkerhetsstrategi - Årlig gjennomgang av IKT sikkerhet (ledelsens gjennomgang)	- Sørge for: - at eget personell har riktige tilganger/ autorisasjoner/roller - behandling av personopplysninger i egen avdeling er meldt til rette instanser - at det er gjennomført obligatorisk sikkerhetsopplæring og at sikkerhetskrav blir overholdt - å gjøre seg kjent med og implementere beredskapsplaner for bortfall av IKT i egen avdeling - at avvik blir behandlet i samsvar med virksomhetens rutiner	- Gjøre seg kjent med og overholde IKT sikkerhetsinstruksen og IKT rutiner - gjennomføre obligatorisk opplæring i informasjonssikkerhet - gjøre seg kjent med og overholde IKT avviksrutiner -	- Sørge for: - at informasjonssystemene oppfyller lovbestemte og andre krav - at informasjonssystemene er tilgjengelig, herunder å utarbeide, inngå og følge opp tjenesteavtale (SLA) om drift og vedlikehold av informasjonssystemene - å etablere ansvarskart for informasjonssystemene - å utarbeide og implementere overordnede beredskapsplaner for IKT - at risikovurderinger blir utført - at risiko overvåkes - å følge opp partnere, leverandør og databehandlere i forhold til sikkerhet	- Overvåke risiko (vurdere, handle, tiltak, varsle, osv..) og at informasjonssystemet benyttes i samsvar med bestemmelser og rutiner - Følge opp IKT sikkerhetsavvik - Utforming av styrende, utførende og kontrollerende IKT sikkerhetsdokument i foretakets Internkontrollsystem - Delta i og kvalitetssikre risikovurderinger - Forberede og følge opp ledergruppens årlige gjennomgang - Gjennomføre sikkerhetsrevisjoner - Delta i regionalt sikkerhetsutvalg - Rapporterer til Dataansvarlig	- Sørge for at det er etablert drift og forvaltningsavtale (ref. SLA) - Sørge for at informasjonssystemet oppfyller lovbestemte og andre krav og er meldt til pålagte instanser - Definere og vedlikeholde tilgangsroller - Sørge for risikovurderinger og overvåke risiko - Følge opp partnere, leverandører og databehandlere i forhold til sikkerhet - Håndtere meldte IKT sikkerhetsavvik - Utarbeide og implementere beredskapsrutiner for bortfall av systemet	- Gi råd og veiledning om behandling av personopplysninger - Føre oversikt over all behandling av personopplysninger - Motta meldinger om behandling av personopplysninger og vurdere om disse er melde- eller konsesjonspliktige - Påse at meldinger/søknader i tilknytning til behandling av personopplysninger blir sendt til aktuelle instanser (unntatt i det som kommer inn under lov om medisinsk og helsefaglig forskning)