

		Utgitt med støtte av: 
Norm for informasjonssikkerhet www.normen.no		
<h1>Opplæring av ledere og medarbeidere</h1>		Støttedokument Faktaark nr 9 Versjon: 2.1 Dato: 15.12.2010

Målgruppe Dette faktaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input checked="" 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 checked="" type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
Ansvar	Virksomhetens ledelse og forskningsansvarlig har ansvaret for å tilrettelegge og sørge for at det gjennomføres opplæring i informasjonssikkerhet og i bruk av de ulike informasjonssystemene.		
Gjennomføring	Gjennomføres ved ansettelse og som en kontinuerlig aktivitet.		
Formål	Formålet med opplæring i informasjonssikkerhet er å gi virksomhetens medarbeidere kompetanse slik at de kan ivareta et godt og hensiktsmessig personvern etter gjeldene krav. Gode opplæringstiltak vil bidra til at ledere og medarbeiderne: <ul style="list-style-type: none"> • Forstår hensikten med og blir i stand til å etterleve et godt personvern. • Blir bevisste på krav i Normen. • Blir oppmerksom på ansvarsforhold i forhold til informasjonssikkerhet. 		
Omfang	Alle virksomheter i helsesektoren skal iverksette tiltak for å lære opp medarbeiderne i informasjonssikkerhet og i bruk av de ulike informasjonssystemene.		
Hjemmel	<ul style="list-style-type: none"> • Personopplysningsforskriften § 2-8 		
Referanser	<ul style="list-style-type: none"> • Norm for informasjonssikkerhet, kapittel 5.6 • NS-ISO 27002 Informasjonsteknologi - Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet 		

Handling/Utførelse

Følgende opplæringstiltak bør gjennomføres:

- Grunnleggende opplæring av ledere
- Grunnleggende opplæring av medarbeidere og studenter
- Løpende opplæringstiltak for vedlikehold av kompetanse

Metodiske tilnærminger og mulige fallgruver

Et styringssystem for informasjonssikkerhet kan oppleves byråkratisk. Samtidig kan det være en utfordring å sette seg inn i rett bruk av informasjonssystemer hvor helse- og personopplysninger behandles. Ofte vil innføring av nye systemer eller funksjoner kreve endringer i arbeidsmåten. Alle disse momentene kan føre til mobilisering av motstand.

Forskning og erfaringer viser at følgende momenter kan forbedre opplæringen:

- Læring oppnås best gjennom egen refleksjon og prøving
- Læring bør inkorporeres i det daglige arbeidet og ikke gjennomføres som en sideaktivitet
- Gjentakelser over tid vil forsterke læringen
- Opplæringen bør ta utgangspunkt i egen arbeidsplass og arbeidssituasjon. Passiv læring gir normalt liten effekt

Nivå og progresjon på opplæring

- Tilpasset opplæring bør legges opp slik at individets rolle og ikke minst kompetanse blir ivaretatt
- Omfanget av et læringsløp for informasjonssikkerhet vil variere med deltagerens behov, forhåndskunnskap og rolle. Erfaringsmessig vil et opplæringsløp, som kan gi varig effekt, ha et tidsforløp på 6 måneder

Materiell

Disse enkle virkemidlene fungerer godt i en opplærings- og bevisstgjøringssituasjon:

- Utarbeid en informasjonsbrosjyre med de viktigste områdene medarbeiderne skal ha kunnskap om. Denne bør deles ut til alle medarbeidere. Nærmeste leder bør følge opp med en samtale omkring temaene som informasjonsbrosjyren tar opp
- Utarbeid, og heng opp plakater med ulike tema på utvalgte steder. Ha illustrasjoner/fotografier fra arbeidssituasjoner i egen virksomhet. Gjenkjennelse har ofte en sterk psykologisk påvirkningskraft. Utvalgte steder kan f.eks. være venterom, ekspedisjoner og personalrom
- Utarbeid ”diskusjonskort” på 15x15 cm med korte beskrivelser av ulike tema i informasjonssikkerhet.

Eksempel

Tabellene nedenfor viser et eksempel på målgruppe, læringsmål og ansvaret for å gjennomføre opplæringen.

	Aktuelle læringsmål for opplæring av ledere	Ansvar
Ledere	<ul style="list-style-type: none">- Bli i stand til å forstå og gi opplæring til medarbeidere i informasjonssikkerhet- Foretakets mål og at sikkerhet er et bidrag til at disse målene kan nås- Ha generell kunnskap om relevante lover og forskrifter, som personopplysningsloven, helseregisterloven, helsepersonelloven og lederens ansvar- Grunnleggende forståelse av virksomhetens kriterier for akseptabel risiko- Ha en oversikt over virksomhetens styringssystem for informasjonssikkerhet- Forstå grunnleggende krav til personvernet og akseptabel forvaltning av helse- og personopplysninger- Ha oversikt over avtaler og prosedyrer der det er gitt tilgang til helsepersonell fra andre virksomheter til virksomhetens helse- og personopplysninger	Hvem: Ansvarlig for informasjonssikkerhet, erfaren leder eller øverste ansvarlige leder. Hvordan: <ul style="list-style-type: none">- Gjennom samtale og veiledning- Selvstudium- Praksis i egen avdeling
Materiell:	Når brukes i læringen:	Finnes:
Styringssystemet i informasjonssikkerhet	Settes seg inn i virksomhetens system	I virksomheten
Personopplysnings- og helseregisterloven Helsepersonelloven Helseforskningsloven	Oversikt over regulatoriske krav	www.lovdatab.no

Medarbeidere	Aktuelle læringsmål for opplæring av medarbeidere	Ansvar
	<ul style="list-style-type: none"> - Forstå grunnleggende kjøreregler for informasjonssikkerhet i virksomheten - Taushetsplikten og grunnleggende prinsipper for et godt personvern - Forstå prosedyrene for innsyn i og endring av helse- og personopplysninger - Plikt, ansvar og metode for å rapportere om avvik på prosedyrer og lovbestemmelser - At tildelt autorisasjon og autentisering er personlig og ikke skal deles med andre - Det er ikke tillatt med fellesbruker ved behandling av helse- og personopplysninger - Viktigheten ved låsing av dører og skap der det oppbevares helse- og personopplysninger - Avlogging eller låsing av PC/arbeidsstasjonen når arbeidsplassen forlades - Aktsomhet for virus ved å ikke åpne ukjente vedlegg i e-post - Aktsomhet for virus ved bruk av Internett - Vær varsom med hensyn til bruk av e-post til helse- og personopplysninger - Ha oversikt over relevante prosedyrer i styringssystemet for informasjonssikkerhet - Forbudet mot urettmessig tilegnelse av journaler (snoking), herunder informasjon om hendelsesregistrering og analyse av hendelsesregistre - Påpasselighet ved samtaler slik at 3.person ikke kan overhøre samtalen - Bruk og sikkerhet i forbindelse med bærbart datautstyr - Informere om konsekvenser og sanksjoner ved sikkerhetsbrudd - Utlevering av helse- og personopplysninger til andre foretak 	<p>Hvem: Personalansvarlig / leder</p> <p>Når</p> <ul style="list-style-type: none"> - Ved ansettelse - I personalmøte - I jobbsamtale - I veiledning - Ved praksis i egen avdeling - På kurs
Materiell:	Når brukes i læringen:	Finnes:
Styringssystemet i informasjonssikkerhet	Sette seg inn i de delene som relevant	I virksomheten
Folder og oppslag med viktige momenter	Grunnleggende og repeterende opplæring	
"Diskusjonskort"	Kollegabasert læring og diskusjon over egen praksis	