



## Datakortet Sikkerhet

### Fagplan 1.0

**Målgruppe:** Brukere av datamaskiner i og utenfor datanettverk i organisasjoner/bedrifter og i hjemmet.

**Mål:** Bevisstgjøre vanlige brukere av datamaskiner på området informasjonssikkerhet. Brukeren skal kjenne til de grunnleggende begreper innenfor informasjonssikkerhet og hva disse betyr i dagligdags utførelse av informasjonsbehandling. Brukeren skal også kjenne til grunnleggende metoder innenfor informasjonssikkerhet og kunne benytte seg av disse. I tillegg skal brukeren være bevisst på hvilke lover, regler og retningslinjer som skal og bør følges i forbindelse med bruk av datamaskiner og informasjonsbehandling.

Kategori	Ref.	Fagområde
1. Informasjons-sikkerhet	1.1	Klassifisering av informasjon. Forstå forskjellen mellom sensitiv informasjon og åpen informasjon. Håndtering av taushetsplikt.
	1.2	Kjenne til hvorfor det er viktig at en organisasjon har en informasjonssikkerhetspolicy.
	1.3	Kjenne til eksempler på sikkerhetshendelser og vanlige brudd på bestemmelser i en organisasjon.
	1.4	Forstå viktigheten av at den enkelte ansatte rapporterer sikkerhetshull, hendelser og svakheter i systemet.
2. Brukerkontroll	2.1	Kjenne til begrepet tilgangskontroll og hvorfor det er nødvendig.
	2.2	Hva menes med brukernavn. Forstå forskjellen mellom brukernavn og passord. Kunne konstruere et sikkert passord. Forstå viktigheten av å endre passord regelmessig, og å holde passordet hemmelig.
	2.3	Forstå viktigheten og konsekvensen av logging/sporing: Pålogging/avlogging, Internettlogging, logging av økonomiske transaksjoner, logging av dokumentopprettelse.
3. Informasjons-håndtering	3.1	Kjenne til overordnet lovverk rundt informasjonshåndtering. Personopplysningsloven, personopplysningsforskriften og offentlighetsloven.
	3.2	Kjenne til forhold rundt lagring av informasjon på sentrale servere/nettverk, som økt tilgjengelighet. Sette adgangsbegrensninger på dokumenter.
	3.3	Vite hva sikkerhetskopi er og hvorfor det er viktig å ta regelmessig sikkerhetskopi. Kjenne til de forskjellige lagringsmedier som brukes til sikkerhetskopi.
	3.4	Være bevisst hvordan sensitiv informasjon skal behandles ved lagring, utskrifter, kopiering og faks.
	3.5	Være bevisst på hvor muntlig informasjonsutveksling i hverdagen foregår. På arbeid, på offentlige plasser, ved kundebesøk, i mobiltelefon.
4. Internett	4.1	Forstå forskjellen på Internett og Intranett.

Kategori	Ref.	Fagområde
	4.2	Kunne endre sikkerhetsinnstillinger i nettleser.
	4.3	Være oppmerksom på sårbarhet ved fast oppkobling til Internett fra hjemmet.
	4.4	Være oppmerksom på problemer omkring kjøp og salg over Internett. Håndtering av personopplysninger og betalingsinformasjon.
	4.5	Kjenne til hva en brannmur er og hva den gjør.
	4.6	Kjenne til hva kryptering er og hvorfor det benyttes.
<b>5. Elektronisk post</b>	5.1	Retningslinjer for sikrere e-post håndtering: E-post fra ukjente, e-post med vedlegg, virusscanning av e-post og kryptering.
	5.2	Kjenne til hva en digital signatur er.
	5.3	Søppelpost (Spam) og følgene av det.
	5.4	Sikkerhetsinnstillinger i e-postprogrammer.
<b>6. Datavirus</b>	6.1	Hva er virus og andre former for ondsinnet kode. Datavirus, dataormer, trojanske hester, Hoax Hvordan virus sprer seg.
	6.2	Kjenne til de mest utbredte filtyper som virus spres gjennom.
	6.3	Beskyttelse mot virus. Nødvendighet av oppdatert anti-virusprogram.
	6.4	Kunne benytte et antivirusprogram for å søke etter og uskadeliggjøre et virus.
	6.5	Sikkerhetsoppdatering av operativsystem, nettleser og e-postprogram.
<b>7. Arbeidsplassen</b>	7.1	Utforming av arbeidsplassen med utgangspunkt i sikkerhet.
	7.2	Bruk av adgangskontroll på arbeidsplassen.
	7.3	Bruk av programvare på arbeidsplassen.
	7.4	Sikkerhet ved arbeid hjemmefra. Oppkobling, lagring og sikkerhetskopiering.
	7.5	Stabil strømforsyning av datamaskiner og nettverk.
	7.6	Kjenne til sårbarhet ved bruk av trådløst tastatur.
<b>8. Mobilt utstyr</b>	8.1	Spesielle hensyn knyttet til lagring og sikkerhetskopiering ved bruk av mobilt utstyr.
	8.2	Håndtering, sikring og merking av mobilt utstyr
	8.3	Være oppmerksom på risiko ved bruk av lånt utstyr og ved avhending av utstyr.
	8.4	Være oppmerksom på sårbarhet ved trådløst nett.
<b>9. Rettigheter og plikter</b>	9.1	Ansattes plikter ved informasjonshåndtering
	9.2	Ansattes rettigheter ved informasjonshåndtering
	9.3	Krav om opplæring i henhold til sikkerhetspolicy.
	9.4	Forstå hva den enkeltes personlige ansvar i forhold til informasjonssikkerhet innebærer.