Sikkerhetsloven

1. **Hvem gjelder loven for?** Sikkerhetsloven gjelder for både offentlige og private virksomheter som er av betydning for nasjonal sikkerhet. Det omfatter også virksomheter som leverer tjenester eller produkter til slike virksomheter. Som lærling kan du derfor bli berørt av loven enten du jobber i en offentlig etat eller for en privat IT-leverandør.
2. **Formål med loven** Sikkerhetsloven skal beskytte nasjonale sikkerhetsinteresser mot trusler som spionasje, sabotasje, terror og annen tilsiktet uønsket hendelse. Som lærling må du vite at IT-systemer ofte inneholder kritisk informasjon som må beskyttes.
3. **Virksomheters ansvar** Alle virksomheter som omfattes av loven har ansvar for å sikre informasjon, systemer og objekter som er viktige for nasjonal sikkerhet. Som lærling kan du bidra gjennom gode rutiner og sikker programmering.
4. **Sikkerhetsstyring** Virksomheter må ha et systematisk arbeid med sikkerhet, kalt sikkerhetsstyring. Det betyr å identifisere risiko, sette i verk tiltak og følge opp. Som lærling er det viktig å kjenne til hvordan man dokumenterer og vurderer risiko i prosjekter.
5. **Klassifisering og merking av informasjon** Informasjon som kan skade nasjonale sikkerhetsinteresser, skal klassifiseres. Du må vite hvordan man behandler og merker informasjon etter sensitivitet, og hvordan du hindrer uautorisert tilgang.
6. **Personellsikkerhet** Personer som får tilgang til sikkerhetsgradert informasjon, må ha godkjent sikkerhetsklarering. Du bør kjenne til at det finnes ulike grader av sikkerhetsklarering, og at ærlighet og pålitelighet er viktig.
7. **Sikkerhetsgraderte systemer** IT-systemer som brukes til å behandle eller lagre sikkerhetsgradert informasjon, må være godkjente. Du bør vite hvordan slike systemer skal utformes og sikres, blant annet med logging, tilgangsstyring og kryptering.
8. **Leverandørers plikter** Også leverandører til sikkerhetsgraderte virksomheter har ansvar etter loven. Hvis du jobber hos en IT-leverandør, kan du bli omfattet av krav til sikkerhetsklarering og sikkerhetsavtaler.
9. **Hendelseshåndtering** Virksomheter skal ha rutiner for å oppdage, varsle og håndtere sikkerhetstruende hendelser. Som lærling bør du vite hvordan slike hendelser oppdages, f.eks. gjennom overvåking, og hvordan man rapporterer dem.
10. **Digital sikkerhet** Digital sikkerhet er en sentral del av loven. Det betyr å beskytte informasjonssystemer mot uautorisert tilgang, manipulering og nedetid. Som lærling bør du kunne grunnleggende prinsipper for cybersikkerhet.
11. **Tilsyn og reaksjoner** Nasjonal sikkerhetsmyndighet (NSM) fører tilsyn med etterlevelse av loven. Det betyr at det kan komme kontroller, og brudd på reglene kan få konsekvenser for virksomheten. Derfor er det viktig å følge retningslinjene og si ifra ved brudd.
12. **Sikkerhetsgradert anskaffelse** Ved anskaffelser som omfatter sikkerhetsgraderte informasjonssystemer, gjelder spesielle krav til sikkerhet. Som lærling bør du vite at

sikkerhet må vurderes tidlig i innkjøpsprosesser, f.eks. ved valg av programvare eller skytjenester.

13. **Informasjonssikkerhet i skyen** Selv om ikke spesifikt nevnt i loven, må prinsippene fra sikkerhetsloven også gjelde når tjenester og data ligger i skyen. Du bør kjenne til hvordan man vurderer leverandører og deres sikkerhetstiltak.
14. **Taushetsplikt og lojalitet** Loven legger til grunn at ansatte og andre med tilgang til sensitiv informasjon har taushetsplikt. Som lærling må du vite at dette gjelder også deg, og at brudd kan få alvorlige konsekvenser.
15. **Varslingsplikt ved sikkerhetsbrudd** Hvis du oppdager noe mistenkelig eller et faktisk sikkerhetsbrudd, har du plikt til å si ifra. Å ignorere slike hendelser kan være alvorlig for virksomheten og for nasjonal sikkerhet.
16. **Integrering av sikkerhet i utviklingsprosesser** I utviklingsarbeid skal sikkerhet være med helt fra planlegging til drift (Security by Design). Som lærling i utvikling er dette viktig for å lage robuste og trygge løsninger.

Oppsummering

Både innen i IT-utvikling og IT-drift bør du ha grunnleggende forståelse for hvordan sikkerhetsloven påvirker arbeidet ditt. Det handler om å beskytte informasjon, systemer og brukere, og om å bidra til å forebygge alvorlige hendelser som kan ramme Norge.