

Sikkerhet i nettverk, datautstyr og tekniske løsning

Konfigurasjonskontroll

Med konfigurasjonskontroll menes at virksomheten (databehandlingsansvarlig) har oversikt over alt utstyr og programvare som benyttes i behandlingen av personopplysninger.

Konfigurasjonskontroll omfatter i denne sammenheng maskinvare (for eksempel PC og server), programvare (for eksempel operativsystem) og nettverket (for eksempel trådløst nettverk).

For eget IT-utstyr som ikke er knyttet til Internett, nettverk eller ekstern e-post er konfigurasjonskontrollen enkel.

Skal virksomheten knytte egen teknisk løsning til Internett og benytte e-post må det etableres tekniske sikkerhetstiltak. Det anbefales å benytte bistand til dette arbeidet. Virksomheten må ha konfigurasjonskontroll for hele løsningen.

Medlemmet må sørge for at den tekniske løsningen (konfigurasjonen) er beskrevet.

Dokumentasjonen skal inneholde:

- sikkerhetsbarrierer (for eksempel brannmur)
- hvor eventuelle servere er plassert
- hvor journalsystemet er plassert
- plassering av arbeidsstasjoner og skrivere
- kryptering av lagringsmedium
- plassering av betalingsterminal(er)
- internettilknytning (inklusive at gjeldende sikkerhetskrav ivaretas)
- tilknytning til andre nettverk
- kryptering av ekstern kommunikasjon

Medlemmet er videre ansvarlig for at konfigurasjonsendringer, dvs. endringer i utstyr og/eller programvare, ikke settes i drift før følgende tiltak er gjennomført:

- risikovurdering som viser at nivå for akseptabel risiko er oppfylt
- test som sikrer at forventede funksjoner er ivaretatt
- implementering som sikrer mot uforutsette hendelser
- ny konfigurasjon er dokumentert

Ansvar for konfigurasjonsendringer kan ivaretas av IT-leverandør dersom medlemmet ikke har kunnskap til å gjøre dette selv.