

## **Analyse af de tekniske og organisatoriske foranstaltninger**

(bruges til udarbejdelse af informationssikkerheds politik)

Foreligger der dokumentation - f.eks. Sikkerhedshåndbog med retningslinjer og politikker?

Er der iværksat adgangsbegrænsning i form af adgangskontrol (fx personlig login)?

Er der styr på rettighedstildeling (autorisation) - oprettelse, rolleskift og nedlæggelse?

Hvem har ansvar for behandling af data i div. situationer?

Foretages der risikovurdering?

Instrueres medarbejderne?

Forefindes der databehandleraftaler?

Er der samme sikkerhed på hjemmearbejdspladser som hos den dataansvarlige?

Forhindres uvedkommende fysisk adgang?

Er der procedurer for reparation og service samt salg og kassation af medier?

Sker den fornødne sletning?

Er der sikring af eksterne kommunikationsforbindelser?

Er der kontrol af tildelte autorisationer inkl. læse, redigere og slette?

Sker der automatisk blokering af afviste adgangsforsøg?

Er der logning af anvendelse af personoplysninger (hvert halve år)?

Er der procedure for håndtering af personoplysninger på papir?

Er der sikring med Firewall og antivirus m.v.?

Har hjemmesideformularer med personoplysninger kryptering?

Laves der kryptering af e-mail med personoplysninger?

Er der procedurer for anmeldelse af og underretning om sikkerhedshændelser?

Anvendes der generelt kryptering og evt. pseudonymisering for at gøre data utilgængelige for uvedkommende?