DIGITALISERINGSSTYRELSEN

Departementets tilsyn med informationssikkerheden på ministerområdet

Denne vejledning om departementets tilsyn med informationssikkerheden på ministerområderne er udviklet på baggrund af regeringens nationale strategi for cyber- og informationssikkerhed af december 2014 med det formål at styrke arbejdet med informationssikkerhed i staten. Digitaliseringsstyrelsen har i tilknytning hertil udarbejdet inspirationsmateriale, der beskriver god praksis for tilrettelæggelse og udførelse af tilsynsopgaven.

Vejledningen er udarbejdet i maj 2015 af Digitaliseringsstyrelsen i samarbejde med en referencegruppe bestående af Justitsministeriet, Forsvarsministeriet, Skatteministeriet, Erhvervs- og Vækstministeriet og med deltagelse af Datatilsynet og Rigsrevisionen som observatører. Vejledningen erstatter "Departementets ansvar for tilsynet med it-anvendelsen i ministerområdet" fra 2005.

Tilsynets formål

Formålet med departementets tilsyn er løbende at vurdere, om styringen af informationssikkerheden i de underliggende institutioner er tilrettelagt hensigtsmæssigt, pålideligt og sikkerhedsmæssigt forsvarligt, så informationers fortrolighed, integritet og tilgængelighed sikres i overensstemmelse med det regelgrundlag, institutionen er underlagt.

Tilsynets omfang

Tilsynet med informationssikkerhed dækker alle institutioner på ministerområdet. Departementet tilrettelægger tilsynets omfang og emner ud fra en vurdering af væsentlighed og risiko.

Tilsynets omfang beror overvejende på institutionernes strategiske, økonomiske og forretningsmæssige betydning for opgavevaretagelsen på ministerområdet.

Hvis der konstateres uregelmæssigheder med styring af informationssikkerheden, eller departementet af andre årsager vurderer, at det er relevant, kan der gennemføres et udvidet tilsyn.

Tilsynets indhold

Indholdet af tilsynet med informationssikkerhed fastlægges på baggrund af det generelle og eventuelle sektorspecifikke regelgrundlag, som ministerområdet er underlagt. Dette omfatter eksempelvis de forpligtelser, der påhviler institutionerne i forhold til efterlevelse af persondataloven, styring af informationssikkerhed efter gældende standard og opfølgning på bemærkninger fra revisions- og tilsynsmyndigheder.

Tilsynet fokuserer særligt på om:

- Institutionens ledelse har tilrettelagt en styring, der sikrer, at informationssikkerheden er fastlagt og håndteret hensigtsmæssigt
- Institutionens generelle it-kontroller sikrer et, efter institutionens forhold, betryggende sikkerhedsniveau
- Institutionen periodisk foretager en risikovurdering af informationssikkerheden for at identificere risiko for tab af fortrolighed, integritet og tilgængelighed

- Institutionen har fastlagt politikker og retningslinjer for informationssikkerheden
- Institutionen har taget stilling til bemærkninger og anbefalinger fra revisions- og tilsynsmyndigheder.

Tilsynets udførelse og opfølgning herpå
Departementets tilsyn med informationssikkerheden på ministerområdet er en integreret del af ledelses- og styringsopgaverne.

Departementet opstiller de overordnede mål for tilsynet og følger op på tilsynsaktiviteterne.

Målene danner baggrund for den konkrete udmøntning af departementets tilsyn.

Tilsynet med informationssikkerheden bygger bl.a. på dialog og samarbejde mellem departementet og ministerområdets institutioner. Udførelsen af tilsynet skal dokumenteres og kan ikke alene baseres på institutionens selvevalueringer.

Tilsynet er begrænset til en vurdering af organisatoriske og administrative forretningsgange samt kontroller på it-området. Tekniske procedurer mv. indgår ikke i tilsynet, men hører hjemme under kontrol- og revisionsaktiviteter.

Vurderingsgrundlaget for tilsynet kan bl.a. sikres ved, at anmode institutionen om følgende informationer:

1. Har de forretningsmæssige aktiviteter givet anledning til væsentlige ændringer i den overordnede informationssikkerhedspolitik?
2. Har risikovurderingen givet anledning til igangsættelse af forbedringstiltag eller væsentlige ændringer?
3. Har driftsstabilitet og tilgængelighed givet anledning til væsentlige overvejelser?
4. Har sikkerhedshændelser i relation til informationssikkerhed givet anledning til væsentlige overvejelser?

Tilsynet afsluttes med en rapportering til departementschefen om resultatet af årets tilsyn med styring af informationssikkerheden.

Bestemmelse om departementets tilsyn skal beskrives i ministerieinstruksen.

Rolle og ansvarsfordeling
Departementet
Departementet er som overordnet myndighed tilsynsansvarlig for det samlede ministerområde, men kan uddelegere tilsynsopgaven til en anden myndighed på ministerområdet, der kompetence- og ressourcemæssigt kan varetage tilsynsfunktionen. Det overordnede tilsyns- og styringsansvar påhviler dog fortsat departementet.

Institutionen
Ansvaret for at varetage informationssikkerheden ligger hos ledelsen i den enkelte institution.