digitaliserings og ligestillingsministeriet

Enhed
Administration og Økonomi

Sagsbehandler
Tobias Christoffer Thykjær

Koordineret med

Sagsnr.

Doknr.
14911

Dato
03-05-2023

Overodnet informationssikkerhedspolitik for Digitaliserings- og Ligestillingsministeriet

Indledning og formål

Formålet med informationssikkerhedspolitikken er at definere en ramme for beskyttelse af ministeriets informationsaktiver og særligt at sikre, at kritiske og følsomme informationssystemer bevarer deres fortrolighed, integritet og tilgængelighed.

Målsætningen for informationssikkerhedspolitikken er at sikre et tilfredsstillende niveau samt at sikre optimale vilkår for informationssikkerheden for hele ministerområdet. Dette skal ske i overensstemmelse med relevante standarder, herunder ISO 27001, og gældende lovgivning, herunder bl.a. databeskyttelsesforordningen, for herigennem at opnå effektivisering og forbedret service samt fastholde ministeriets troværdighed, beskytte de registreredes rettigheder og sikre en effektiv og kontinuerlig sagsbehandling af høj kvalitet.

Hensigten med sikkerhedspolitikken er at tilkendegive over for alle, som har en relation til ministeriet, at anvendelse og tilgang til informationsaktiverne er underkastet denne sikkerhedspolitik, sikkerhedshåndbøger, politikker og retningslinjer, der måtte være fastlagt i de enkelte institutioner.

Omfang

Den overordnede informationssikkerhedspolitik for ministeriet dækker følgende institutioner:

- Digitaliserings- og Ligestillingsministeriets departement
- Danmarks Statistik
- Digitaliseringsstyrelsen

Desuden er følgende råd og nævn omfattet af politikken:

- Digitaliseringsrådet
- Cybersikkerhedsrådet

Politikken omfatter ministeriets informationer, som er enhver information, der tilhører ministeriet samt informationer, som ikke tilhører ministeriet, men som ministeriet kan gøres ansvarlig for. Dette inkluderer f.eks. alle data om personale, data om finansielle forhold, alle data som bidrager til administrationen af ministeriet, produktions- og sagsbehandlingsdata, anlægsdata samt informationer som er overladt ministeriet af andre.

Politikken omfatter alle ministeriets informationer, ligegyldigt hvilken form de opbevares i og formidles på.

Politikken gælder ligeledes for alle ansatte uden undtagelse, både fastansatte og personer, som midlertidigt arbejder for ministeriet, herunder konsulenter. Alle disse personer bliver i dette dokument betegnet som "medarbejdere". Ved udlicitering af dele af eller hele it-driften skal det i samarbejdet med serviceleverandøren sikres, at ministeriets sikkerhedsniveau opfyldes, således at serviceleverandøren, dennes faciliteter og de medarbejdere, som har adgang til ministeriets informationer, lever op til ministeriets informationssikkerhedsniveau.

Informationssikkerheden omfatter alle fysiske, logiske og organisatoriske tiltag i relation til informationsaktiverne og har til formål at beskytte alle former for forretningsrelateret information mod tilsigtede eller utilsigtede, interne eller eksterne hændelser, som kan medføre tilintetgørelse, forvanskning, forringelse eller misbrug af data, brud på informationers fortrolighed og integritet eller hindring af tilgængelighed.

Sikkerhedsniveau

Det er væsentligt for ministeriet at beskytte informationsaktiver og udelukkende tillade brug, adgang og offentliggørelse af informationer i overensstemmelse med fastlagte retningslinjer og procedurer herfor og under hensyntagen til vedtagne standarder og gældende lovgivning.

Den enkelte institution skal én gang årligt gennemføre en overordnet risikovurdering af institutionens kritiske systemer, således at ledelsen i institutionen kan holde sig informeret om det aktuelle risikobillede. Der skal ligeledes foretages en risikovurdering ved større forandringer i organisationen.

Institutionerne fastlægger på baggrund af denne risikovurdering og en konkret sandsynligheds- og konsekvensanalyse et sikkerhedsniveau, som svarer til betydningen af informationsaktiverne. Alle institutioner skal som minimum endvidere implementere et ISO 27001 baseret ledelsessystem for informationssikkerhed, ISMS (Information Security Management System) og tage stilling til kontrollerne i standardens Anneks A i form af en overensstemmelseserklæring, SoA (Statement of Applicability).

Sikkerhedsbevidsthed

Informationssikkerhed vedrører ministeriets samlede informationer, og gennemførelse af en informationssikkerhedspolitik kan ikke foretages af ledelsen alene. Alle medarbejdere og samarbejdspartnere har ligeledes et ansvar for at bidrage til at beskytte ministeriets informationsaktiver.

Som brugere af ministeriets informationsaktiver skal alle medarbejdere følge informationssikkerhedspolitikken og øvrige retningslinjer for informationssikkerhed. Medarbejderne må kun anvende ministeriets informationer som led i det arbejde, de udfører, og de forpligter sig til at beskytte informationerne i overensstemmelse med informationernes klassifikation.

Det er ligeledes afgørende, at informationssikkerheden løbende integreres i alle forretningsgange, driftsopgaver og projekter.

Brud på informationssikkerheden

Såfremt en medarbejder opdager trusler mod informationssikkerheden eller brud på denne, skal dette straks meddeles til den lokale it-sikkerhedskoordinator/leder eller institutionens HR-chef samt databeskyttelsesrådgiveren, såfremt der er tale om mere personfølsomme sager.

Involverer et brud på informationssikkerheden personoplysninger, vil der ligeledes være tale om et brud på persondatasikkerheden, som skal håndteres efter databeskyttelsesforordningens og databeskyttelseslovens bestemmelser.

De enkelte institutioner skal lokalt indføre passende sanktionering af og procedurer ved overtrædelser af informationssikkerheden eller deraf afledte retningslinjer i overensstemmelse med gældende personalepolitik og øvrig lovgivning.

Tilsyn med informationssikkerheden

Departementet fører tilsyn med institutionerne med henblik på løbende at vurdere, om styringen af informationssikkerheden i institutionerne er tilrettelagt hensigtsmæssigt, pålideligt og sikkerhedsmæssigt forsvarligt, så informationers fortrolighed, integritet og tilgængelighed er sikret i overensstemmelse med det regelgrundlag, som institutionen er underlagt.

Departementet tilrettelægger tilsynets omfang og emner ud fra en vurdering af væsentlighed og risiko, og tilsynet vil i øvrigt ske inden for rammerne af Digitaliseringsstyrelsens vejledning på området.

Løbende erfaringsudveksling og koordination

Med henblik på at understøtte erfaringsudveksling og koordination af informationssikkerhedsarbejdet i ministeriet, er der oprettet en Decentral Cyber- og Informationssikkerhedsenhed (DCIS), der er organisatorisk placeret i Digitaliseringsstyrelsen. DCIS har ansvar for at vidensdele og koordinere emner, der vedrører cyber- og informationssikkerhed, og som relaterer sig til DCIS-arbejdet.

Der etableres et koordinerende udvalg for informationssikkerhedskoordinatorer (ISKU) på ministerområdet. ISKU har til formål at kunne bruges til vidensdeling, koordination, udmøntning af initiativer i Cyber- og informationssikkerhedsstrategien og drøftelser vedr. kompetencegivende tiltag, mv. Derudover kan spørgsmål og sager om informationssikkerhed behandles på bilaterale møder mellem institutionernes direktion og departementet.

Digitalisering- og Ligestillingsministeriet, den 4. maj 2023