Styrelsen for Dataforsyning og Effektivisering

Kontor
Metode og Teknologi

Dato. 22. juni 2020

J nr. 1209-0004

/ RA

Informationssikkerhedspolitik for Styrelsen for Dataforsyning og Effektivisering

Baggrund

Styring af informationssikkerheden er en vigtig opgave for statens institutioner, og regeringens Økonomiudvalg vedtog derfor i 2010, at statens institutioner skal følge den internationale standard for styring af informationssikkerheden ISO 27001. Derfor og fordi data, informationer og it-systemer spiller en vigtig rolle for opgavevaretagelsen, efterlever Styrelsen for Dataforsyning og Effektivisering (herefter benævnt "Styrelsen") den internationale standard.

Informationssikkerhedspolitikken udgør rammen og angiver den målsætning, hvorpå informationssikkerheden i Styrelsen skal baseres.

Informationssikkerhedspolitikkens formål

Data, informationer og it-systemer udgør en stor og vigtig del af Styrelsens aktiver og er grundlæggende nødvendige for at kunne varetage myndighedsopgaven og realisere forretningsmæssige målsætninger.

Styrelsen arbejder med store mængder af data, som dels tilvejebringes og tilgængeliggøres for omverdenen, og dels anvendes i varetagelsen af myndighedsopgaverne. Styrelsen er afhængig af et godt omdømme i omverdenen og fortsat tillid, og derfor skal informationssikkerhedspolitikken sikre, at data og informationer behandles i overensstemmelse med de krav, der stilles til organisationer med stor samfundsmæssig betydning. Styrelsens data, deres karakter og anvendelse betyder, at sikring af integritet og tilgængelighed har høj prioritet. For så vidt angår behandlingen af personoplysninger, grunddata og andre samfundsrelevante data, forventer

Styrelsen for Dataforsyning og Effektivisering

Rentemestervej 8
2400 København NV

T: 72 54 55 00
E: sdfe@sdfe.dk

www.sdfe.dk

fx borgere, virksomheder og andre myndigheder med rette, at vi tillige sikrer en høj grad af fortrolighed.

Styrelsen ser et højt informationssikkerhedsniveau som en af flere vigtige forudsætninger for at kunne overholde lov- og myndighedskrav og en kvalitetsfaktor i forhold til at kunne tilbyde sikker opgaveløsning over for minister, samarbejdspartnere, andre myndigheder, private virksomheder og borgere.

Styrelsen har som mål, at styringen af informationssikkerheden vedvarende vedligeholdes og forbedres, der hvor det findes nødvendigt.

Omfang og gyldighedsområde

Informationssikkerhedspolitikken omfatter alle data og informationer, som Styrelsen kan gøres ansvarlig for, uanset hvilken form de opbevares og kommunikeres på.

Informationssikkerhedspolitikken henvender sig til alle ansatte (uanset ansættelsesform) i Styrelsen og til relevante eksterne parter med fysisk eller logisk adgang til Styrelsens systemer, informationer og data. Krav til leverandører og konsulenter skal konkretiseres i aftaleforholdet.

Risikovurdering og -håndtering - sikkerhedsniveau

Informationssikkerhedspolitikken sætter rammerne for sikkerhedsniveauet i Styrelsen. Sikkerhedsniveauet fastlægges på baggrund af periodiske vurderinger af forretningsmæssige informationssikkerhedsrisici, som styrelsen ønsker at håndtere.

Informationssikkerheden skal tilrettelægges således, at større eller væsentlige drifts- og sikkerhedshændelser undgås, samtidig med at der tages hensyn til at minimere belastningen af ressourcer til sikkerhedskontroller. Dette skal opnås gennem risikostyringen og den periodiske risikovurdering af styrelsens informationsaktiver.

Informationssikkerhedspolitikken skal grundlæggende sikre, at de data og informationer, som Styrelsen kommunikerer til borgere, samarbejdspartnere, offentlige myndigheder og private virksomheder samt internt i ministeriets koncern, er **tilgængelige**, forbliver **fortrolige**, når de er vurderet som værende af fortrolig karakter, og er korrekte.

Ledelsen fastlægger herigennem et sikkerhedsniveau, der lever op til følgende mål:

- Der skal som minimum en gang årligt gennemføres it-risikovurderinger.

- Data og informationer skal beskyttes mod uautoriseret fysisk og logisk adgang.
- Data og informationer skal sikres mod tab af fortrolighed og integritet.
- Medarbejdere skal trænes for at sikre at denne informationssikkerhedspolitik samt regler og procedurer af informationssikkerhedsmæssig art efterleves.
- Der skal styres og følges op på leverandører til sikring af stabil og sikker drift samt af styrelsens data og informationer, som leverandører har adgang til.
- Der skal etableres et it-beredskab, der sikrer fokuseret styring af retablering af systemer og data og adgang til disse. Der skal endvidere etableres nødplaner, der sikrer den fortsatte afvikling af forretningsservices.
- Der skal sikres efterlevelse af centralt udstukne retningslinjer, national lovgivning samt EU-lovgivning.
- Den anerkendte standard for styring af informationssikkerhed, ISO/IEC 27001 skal efterleves.
- Ledelsessystemet til styring af informationssikkerheden (ISMS) skal løbende revurderes med henblik på at opnå stadige forbedringer af ledelsessystemet og informationssikkerheden.
- Der skal gennemføres monitorering og rapportering af sikkerhedshændelser.

Disse intentioner skal understøttes af et tilhørende sæt af politikker, retningslinjer, kontroller, procedurer og vejledninger. Det skal desuden sikres, at intentionerne konkretiseres i fremadrettede handlingsplaner i leverandøraftaler og databehandleraftaler.

Sikkerhedsbevidsthed

Alle medarbejdere har et ansvar for at medvirke til at beskytte data, informationer og it-systemer. Alle medarbejdere skal derfor dels i forbindelse med og igennem ansættelsen være orienterede om det generelle sikkerhedsniveau samt de retningslinjer, som er specifikke for den enkeltes opgaveløsning. Som leder har man ansvar for at sikre, at medarbejderne efterlever de udstukne politikker, retningslinjer og procedurer for informationssikkerhed. Det er ledelsens mål, at der løbende følges op, sådan at sikkerhedsbevidstheden hos alle medarbejdere vurderes, vedligeholdes og forbedres for at kunne opretholde det ønskede sikkerhedsniveau. Det er et mål, at informationssikkerhed integreres i alle Styrelsens processer, således at kravene efterleves som en naturlig del af arbejdet.

Dispensation fra informationssikkerhedspolitikken

Dispensation fra informationssikkerhedspolitikken og de tilhørende politikker, retningslinjer, kontroller, procedurer og vejledninger kan eventuelt imødekommes på

baggrund af en risikovurdering og implementering af eventuelle nødvendige kompenserende sikringsforanstaltninger. Dispensationer skal godkendes af ledelsen, inden aktiviteterne kan gennemføres og tillige dokumenteres.

Brud på informationssikkerheden

Hvis en medarbejder har mistanke om eller kan konstatere brud på informationssikkerheden eller opdager forhold der eventuelt kan føre til det, skal dette rapporteres til informationssikkerhedskoordinatoren eller nærmeste leder, som har ansvar for at rapportere forholdet til informationssikkerhedskoordinatoren.

Overtrædelse af informationssikkerhedspolitikken og de udstukne politikker, retningslinjer, kontroller, procedurer og vejledninger behandles efter de gældende personaleretlige regler og styrelsens personalepolitik.

Godkendelse og kommunikation

Informationssikkerhedspolitikken for Styrelsen godkendes af ledelsen og revurderes årligt eller, hvis risikobilledet ændres eller i forbindelse med større organisatoriske ændringer m.v.

Informationssikkerhedspolitikken kommunikeres til alle styrelsens ansatte på intranettet og i arkitekturportalen og til eksterne parter på styrelsens hjemmeside. Informationssikkerhedspolitikken kan vedhæftes kontrakter og andre relevante aftaledokumenter med eksterne parter.

Informationssikkerhedspolitikken træder i kraft den 22. juli 2020 og erstatter den tidligere godkendte informationssikkerhedspolitik.