Styrelsen for Dataforsyning og Effektivisering

Notat om

Kontor
Metode og Teknologi

Dato
11. februar 2016

J nr.

/ CHL /RA

Informationssikkerhedspolitik for Styrelsen for Dataforsyning og Effektivisering

Baggrund

Styring af informationssikkerheden er en vigtig opgave i statens institutioner, og regeringens Økonomiudvalg vedtog derfor i 2010, at statens institutioner skal følge den internationale standard for styring af informationssikkerheden ISO 27001 fra 2013. Derfor og fordi data, informationer og it-systemer spiller en vigtig rolle for opgavevaretagelsen, efterlever Styrelsen for Dataforsyning og Effektivisering 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 Styrelsen for Dataforsyning og Effektiviserings ressourcer og er grundlæggende nødvendige for at kunne varetage myndighedsopgaven og realisere forretningsmæssige målsætninger.

Styrelsen for Dataforsyning og Effektivisering arbejder med store mængder af data, som dels produceres og tilgængeliggøres for omverdenen, og dels anvendes i vores myndighedsopgaver. Styrelsen er afhængig af et godt omdømme i omverdenen og fortsat tillid. Derfor skal informationssikkerhedspolitikken sikre, at data og informationer behandles i overensstemmelse med de krav, der stilles til organisationer med stor samfundsmæssig betydning. Styrelsen for Dataforsyning og Effektiviserings data, deres karakter og anvendelse betyder at sikring af integritet og tilgængelighed har høj prioritet. For personfølsomme oplysninger og på en række andre områder, forventer fx borgere, virksomheder og andre myndigheder med rette, at vi tillige sikrer fortrolighed af data.

Styrelsen for Dataforsyning og Effektivisering 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 for Dataforsyning og Effektivisering

Rentemestervej 8
2400 København NV

T: +45 72 54 55 00

www.sdfe.dk

Styrelsen for Dataforsyning og Effektivisering 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 for Dataforsyning og Effektivisering kan gøres ansvarlig for. Informationssikkerhedspolitikken og informationssikkerhedsarbejdet i styrelsen skal overholde retningslinjerne udstukket i den koncernfælles informationssikkerhedspolitik for Energi-, Forsynings- og Klimaministeriet.

Informationssikkerhedspolitikken henvender sig til alle ansatte (uanset ansættelsesform) i Styrelsen for Dataforsyning og Effektivisering og til relevante eksterne parter med fysisk eller logisk adgang til styrelsens systemer 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 for Dataforsyning og Effektivisering 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 fremstår med **korrekt** indhold.

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

- Der skal som minimum en gang årligt gennemføres it-risikovurderinger.
- Data skal beskyttes mod uautoriseret fysisk og logisk adgang.
- Data skal sikres mod tab af fortrolighed og integritet.
- Medarbejdere skal trænes for at sikre efterlevelse af denne informationssikkerhedspolitik.

- Der skal styres og følges op på leverandører til sikring af stabil og sikker drift.
- Der skal etableres it-beredskab, der sikrer fokuseret styring mod adgangen til og retablering af systemer og data, så vidt muligt. Samt nødplaner der sikrer den fortsatte afvikling af forretningsprocesser.
- Der skal sikres efterlevelse af centralt udstukne retningslinjer, national lovgivning samt EU-direktiver/-forordninger, indtil de er omsat i dansk lovgivning.
- Den anerkendte standard for styring af informationssikkerhed, ISO/IEC 27001:2013 skal efterleves.
- Der skal gennemføres revurderinger af ledelsessystemet til styring af informationssikkerheden (ISMS) med henblik på vedvarende forbedring af ledelsessystemet og informationssikkerheden.
- Der skal gennemføres monitorering og rapportering af sikkerhedshændelser.

For at understøtte disse intentioner skal der være beskrevet passende politikker, procedurer og eventuelt vejledninger. Det skal desuden sikres, at ovenstående intentioner konkretiseres i fremadrettede handlingsplaner og i leverandøraftaler.

Sikkerhedsbevidsthed

Alle medarbejdere har et ansvar for at bidrage til at beskytte data, informationer og informationssystemer. 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 enkelte medarbejders opgaver. Dels er det ledelsens mål, at der løbende følges op, således at sikkerhedsbevidstheden hos medarbejderne vurderes, vedligeholdes og forbedres for at kunne opretholde det ønskede sikkerhedsniveau. Det er et mål, at informationssikkerheden integreres i alle Styrelsen for Dataforsyning og Effektiviserings processer, således at kravene på sigt efterleves som en naturlig del af arbejdet.

Dispensation fra informationssikkerhedspolitikken

Dispensation fra informationssikkerhedspolitikken og de tilhørende retningslinjer kan eventuelt imødekommes på baggrund af en risikovurdering og eventuelt implementering af nødvendige kompenserende sikringsforanstaltninger. Dispensationer skal godkendes af ledelsen, inden handlingerne kan gennemføres og tillige dokumenteres.

Brud på informationssikkerheden

Hvis en medarbejder har mistanke om, eller kan konstatere brud på informationssikkerheden, skal dette rapporteres til den informationssikkerhedsansvarlige eller

nærmeste leder, som har ansvar for rapportering til den informationssikkerhedsansvarlige.

Overtrædelse af informationssikkerhedspolitikken og de heraf afledte retningslinjer behandles efter de gældende personaleretlige regler og styrelsens personalepolitik.

Godkendelse og kommunikation

Informationssikkerhedspolitikken for Styrelsen for Dataforsyning og Effektivisering godkendes ledelsen og revurderes en gang om året på baggrund af opdaterede risikovurderinger eller i forbindelse med større organisatoriske ændringer m.v.

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

Godkendt den 15-02-2016

(Søren Reeberg Nielsen, vicedirektør)