DANMARKS STATISTIK

Danmarks Statistiks informationssikkerhedspolitik

Vi passer godt på data i en digital verden

Danmarks Statistik er den centrale statistikproducent i Danmark og har mange års erfaring med at behandle data til brug for belysning af samfundsforholdene. Danmarks Statistik opererer på et sæt af kerneværdier, som er uafhængighed, troværdighed, brugerorientering og datasikkerhed.

I overensstemmelse hermed, og for at værne om den digitale tillid, som samfundet viser os, har vi et vedblivende og skarpt fokus på informationssikkerheden. Den informationsteknologiske udvikling resulterer i en voldsomt stigende mængde af data. I Danmarks Statistik foregår der et tilsvarende kontinuert arbejde med at udvikle de procedurer og sikringsmekanismer, som vi har sat op omkring data. Befolkningen og brugerne af vores tjenester skal fortsat kunne have tillid til, at data er i sikre hænder.

Danmarks Statistik marts 2020

Jørgen Elmeskov
Rigsstatistiker

Indhold

1 Indledning

Dette er Danmark Statistiks (DSTs) informationssikkerhedspolitik, som fastsætter rammerne for arbejdet med sikkerhed i DST, og som følger den statslige informationssikkerhedsstandard ISO 27001.

I øvrigt henvises til Social- og Indenrigsministeriets overordnede informationssikkerhedspolitik som gælder for hele ministeriets ressortområde.

Ordet informationssikkerhed skal forstås bredere end datasikkerhed og er en anvendt term i statens sikkerhedshåndtering. Med informationssikkerhed forstås den nødvendige beskyttelse af samtlige ressourcer, der indgår i eller bidrager til DSTs behandling og kommunikation af information, uanset om det er i elektronisk form, i papirform mm. – herunder også teknologi og organisatoriske processer.

DSTs informationssikkerhedspolitik bygger på de krav, som er identificeret på grundlag af:

- DSTs til enhver tid gældende strategi, pt. Strategi 2022
- Forskrifter, lovgivning/forordninger og direktiver mv. inden for DSTs område, herunder ISO 27001 samt Databeskyttelsesforordningen (GDPR)
- Det nuværende og forventede trusselsmiljø vedrørende informationssikkerhed.

DST skal på baggrund af systematiske risikovurderinger og en konkret sandsynligheds-og konsekvensanalyse sikre det sikkerhedsniveau, som DSTs Direktion har besluttet og som svarer til værdien af informationsaktiverne i DST. Desuden har DST implementeret et ISO 27001 baseret ledelsessystem for informationssikkerhed, ISMS (Information Security Management System) og har taget stilling til kontrollerne i standardens Anneks A i form af en overensstemmelseserklæring, SoA (Statement of Applicability), der er udvidet med et sæt af specifikke DST-kontroller.

Informationssikkerhedspolitikken skal skabe rammerne for en række konkrete regler, retningslinjer og procedurer, som indeholder et effektivt kontrolmiljø. Dermed etableres et grundlag for det daglige arbejde med informationssikkerhed i for DST.

Informationssikkerhedspolitikken er en vigtig del af DSTs informationssikkerhedshåndbog og beskriver det ledelsesgodkendte niveau for sikkerhed.

DSTs informationssikkerhedspolitik beskriver vigtigheden af arbejdet med informationssikkerhed i DST og fastlægger ambitionsniveauet herfor. Informationssikkerhedspolitikken indeholder derfor de overordnede sikkerhedsmålsætninger og danner grundlag for udformning af DSTs informationssikkerhedshåndbog, der skal forstås som fællesbetegnelsen for informationssikkerhedspolitikken med de underliggende regelsæt og procedurer.
DSTs vigtigste dokumenter og politikker vedr. informationssikkerhed af ekstern interesse (inkl. nærværende informationssikkerhedspolitik) publiceres også på DSTs hjemmeside og befinder sig pt. på http://www.dst.dk/da/OmDS/lovgivning/.

2 Målsætningerne for informationssikkerhed i DST

Det er DSTs mål at opretholde et højt informationssikkerhedsniveau, der som minimum er på samme niveau som sammenlignelige institutioners. Målsætningen om et højt sikkerhedsniveau afvejes med ønsket om en hensigtsmæssig og brugervenlig anvendelse af it og øvrige økonomiske ressourcer.

Kravene til informationssikkerhed vurderes i forhold til deres relevans for DST, og hermed holdes fokus på et informationssikkerhedsniveau, hvor god sund fornuft samt hensynet til offentlighedens berettigede behov og forventning om en sikker forvaltning af data og aktiver er en afgørende faktor. Desuden skal data og systemer sikres ud fra en vurdering af, hvad der er nødvendigt under hensyntagen til de økonomiske rammer.

Målet for informationssikkerheden er derfor at:

- Opnå mulighed for fortrolig behandling, transmission og opbevaring af data, bl.a. ved brug af afidentificering/pseudonymisering og kryptering af data i størst muligt omfang.
- Opnå høj driftssikkerhed og minimal risiko for større nedbrud
- Understøtte overholdelsen af Databeskyttelsesforordningen (GDPR), også som databehandler for andre
- Forhindre datatab og - lækager
- Forhindre identifikation af enkeltpersoner og enkeltmandsvirksomheder, bl.a. gennem afidentificering og diskretionering
- Forhindre svig og bedrageri gennem automatiserede og manuelle kontrolforanstaltninger
- Og i forlængelser heraf, opnå korrekt funktion af it-systemerne med minimeret risiko for manipulation af data og systemer. Dvs. at faciliteter hertil skal være til stede og benyttes efter konkret behov
- Sikre mod forsøg på tilsidesættelse af sikringsforanstaltninger
- Understøtte bevidstheden om informationssikkerhed internt og eksternt, således at alle medarbejdere og eksterne brugere er opmærksomme på og forholder sig til informationssikkerhed i det daglige arbejde

DST ser ikke kun et højt sikkerhedsniveau som et krav for at kunne overholde lov- og myndighedskrav, men også som et kvalitetselement for at kunne tilbyde en sikker service for borgerne og indberetterne af data. Informationssikkerhed er med andre ord en eksplicit nøgleværdi af strategisk karakter hos DST, der også indgår som selvstændigt område i Strategi 2022. Informationssikkerhed skal med andre ord være en naturlig del af it-aktiviteterne i DST.

3 Politikkens omfang

Informationssikkerhedspolitikkens scope og omfang defineres således:

- Informationssikkerhedspolitikken gælder for alle ansatte i DST uanset ansættelsesform, herunder også eksterne konsulenter og servicemedarbejdere.
- Informationssikkerhedspolitikken gælder for alle systemer og alle data i DSTs besiddelse.
- Leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til DSTs systemer og data, skal ligeledes have kendskab til og følge informationssikkerhedspolitikken.
- Informationssikkerhedspolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af DSTs it-systemer, data og papirarkiver.

- Informationssikkerhedspolitikken godkendes af Direktionen og revurderes en gang årligt for at sikre, at den er i overensstemmelse med de sikkerhedsmålsætninger, som DST arbejder efter.

4 Overtrædelse af politikken

Alle medarbejdere i DST er forpligtet til at efterleve den gældende informationssikkerhedspolitik med tilhørende retningslinjer, forretningsgange og relaterede bilag. En overtrædelse kan, efter omstændighederne, medføre sanktioner.

Hvis en medarbejder er vidende om, at DSTs informationssikkerhed overtrædes, skal det meddeles til informationssikkerhedskoordinatoren, direktøren for Brugerservice eller Servicedesk hurtigst muligt. Afhængigt af situationen kan der komme personalemæssige konsekvenser.

5 Organisation og ansvar

Direktionen er ansvarlig for at arbejde med informationssikkerhed på et strategisk niveau, således at informationssikkerhedsmæssige overvejelser inddrages i alle væsentlige beslutninger. Ledere og medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for sikkerhed i det daglige arbejde.

Planlægningen, implementeringen af og kontrollen af informationssikkerheden er defineret af DSTs ledelse (Direktionen). Informationssikkerhedskoordinatoren er ansvarlig for implementering og vedligeholdelse af informationssikkerhedssystemet i DST og er ansvarlig for opfølgning på sikkerhedshændelser.

Informationssikkerhedspolitikken skal revurderes, ajourføres og godkendes en gang om året af Direktionen, eller i forbindelse med eventuelle situationer, der tilsiger det, såsom større ressortændringer.

DST har nedsat et informationssikkerhedsudvalg med reference til Direktionen. Formand for udvalget er en afdelingsdirektør (for Brugerservice) og de øvrige medlemmer repræsenterer alle afdelinger samt IT.

DST har en informationssikkerhedskoordinator, som er personalemæssigt placeret i IT, men i informationssikkerhedsmæssige spørgsmål refererer til formanden for informationssikkerhedsudvalget. Det løbende daglige informationssikkerhedsarbejde varetages af IT og it-sikkerhedsgruppen, som understøttes af DSTs governancemodel på sikkerhedsområdet.

DST har udpeget systemejere, som er de fagligt ansvarlige for DSTs systemer. Systemejerne er typisk cheferne i IT samt kontorchefer for statistikkontorerne. De skal sikre, at de gældende informationssikkerhedsregler overholdes for deres systemer.

Alle medarbejdere er personligt ansvarlige for at overholde DSTs informationssikkerhedsregler og skriver under herpå ved ansættelsen.

6 Sikkerhedsbevisthed

Alle medarbejdere i DST har ansvar for informationssikkerheden. De skal være bekendte med og efterleve DSTs informationssikkerhedspolitik, informationssikkerhedshåndbog, regler og procedurer i DST.

Den nødvendige viden og kompetence omkring informationssikkerhed skal kommunikeres til alle medarbejdere, og der skal løbende arbejdes med hold-

ninger, kultur og viden omkring informationssikkerhed; dette skal ske i forbindelse med ansættelsen, ved intro-kurser samt løbende i form af jævnlige awareness-kampagner.

7 Datafortrolighedspolitik

Fortrolighed i omgangen med statistikprodukter og andre datamaterialer drejer sig om at sikre statistikkens enheder mod en spredning af oplysninger om fortrolige forhold. Det gælder såvel i forhold til omverdenen som i forhold til medarbejderne i Danmarks Statistik.

Reglerne til håndhævelse af datafortroligheden er udmøntet i en datafortrolighedspolitik med tilhørende retningslinjer for videregivelse og diskretionering samt fastlæggelse af individuelle adgangsrettigheder til fortrolige oplysninger i Danmarks Statistik. Datafortrolighedspolitikken er forankret i Datafortrolighedsudvalget.

8 Informationssikkerhedshåndbogen

Informationssikkerhedspolitikken er uddybet i et sæt retningslinjer og forretningsgange. Tilsammen udgør politikken, retningslinjer, beredskabspolitik og forretningsgange informationssikkerhedshåndbogen.

De retningslinjer, der er relevante for medarbejderne i DST, findes tilgængelige på intranettet. Derudover findes et sæt retningslinjer, som er relevante for it-medarbejderne og som befinder sig på et netværksdrev, der er tilgængeligt for it-medarbejderne.

Det daglige operationelle ansvar for at vedligeholde informationssikkerhedshåndbogen befinder sig hos informationssikkerhedskoordinatoren og it-sikkerhedsgruppen i IT. Materiale hørende til informationssikkerhedshåndbogen godkendes i informationssikkerhedsudvalget, der som nævnt har reference til Direktionen.

Det er informationssikkerhedskoordinatorens ansvar at styre den dokumentation, der indgår i DST informationssikkerhedshåndbog eller på anden vis understøtter ledelsessystemet for informationssikkerheden i DST, herunder sikre at der foretages regelmæssig gennemgang og opdatering af dokumenterne.

9 Sikkerhedsniveau

Uafhængighed, troværdighed, datasikkerhed og brugerorientering er kerneværdier for DST. Datasikkerhed er et vigtigt strategisk indsatsområde.
Et tilstrækkeligt informationssikkerhedsniveau opnås igennem sikringsforanstaltninger, der sikrer:

1. Fortrolighed, integritet/ autenticitet (uafviselighed) og tilgængelighed af DSTs systemer og data i forhold til den it-risikovurdering, der er fastsat for det enkelte system / sæt af data:

   Fortrolighed: DST skal løbende sikre, at indsamlede data bliver behandlet sikkert. DST skal sikre mulighed for sikker behandling, transmission og opbevaring af data samt forhindre tab af data. Sikkerhedsforanstaltningerne skal beskytte data mod misbrug, og mod at nogen uberettiget får adgang til oplysninger om enkeltpersoner og virksomheder. I forlængelse heraf har DST som strategisk mål at anvende afidentificerede data i størst muligt omfang.

Integritet: DST arbejder løbende på at sikre en pålidelig og korrekt funktion af systemerne med minimeret risiko for ukorrekt datagrundlag og dermed statistik f.eks. som følge af menneskelige og systemmæssige fejl. Derfor skal der løbende arbejdes med at sikre, at DSTs dokumentation og test af systemerne er af høj kvalitet.
Tilgængelighed: DST arbejder løbende på at opnå en høj tilgængelighed med høje oppetider og minimeret risiko for nedbrud. DST arbejder jf. Strategi2022 i højere og højere grad digitalt. Det gælder både i forhold til ydelser, processer, data og statistiksamarbejde. Derfor er systemernes tilgængelighed af stigende strategisk betydning. Niveauet for systemernes tilgængelighed besluttes af direktionen.

2. Beskyttelse af DSTs it-aktiver, medarbejdernes kompetencer, organisationens image og informationer/data i DSTs varetægt.

For at fastholde det tilstrækkelige sikkerhedsniveau i DST skal følgende overholdes:

- Der skal forefindes retningslinjer og forretningsgange, som sikrer, at informationssikkerhed er en integreret del af DSTs drift og daglige arbejde.
- DST skal i sin kontrakt- og leverandørstyring sikre, at brugen af eksterne konsulenter, samarbejdspartnere og leverandører lever op til DSTs informationssikkerhedsniveau.
- Der skal ske opfølgning på informationssikkerheden – se nærmere under afsnit 13 ”Opfølgning”.

10 Risikovurdering og klassifikation

Det er DSTs politik at have en risikobaseret tilgang til informationssikkerhed jf. ISO 27001. Det vil sige, at DST forholder sig aktivt til hvilke risici, der eksisterer og beslutter hvilke tiltag, der skal imødegå risici.

Den forretningsmæssige risikovurdering
Informationssikkerheden i DST skal tilgodese lov- og myndighedskrav, kontraktlige forpligtelser samt forpligtelser overfor de aktører, der er forpligtigede til at anvende DST. Det er DSTs målsætning at være bevidst om relevante risici, og forholde sig til disse set i lyset af økonomiske forhold.

Der foretages årligt et antal risikovurderinger af de mest kritiske systemer, dvs. de forretningskritiske og samfundskritiske systemer, efter nærmere aftale med ledelsen (Informationssikkerhedsudvalget), samt ved eventuelle større ændringer i opgaver, leverandører, it-systemer eller anvendelsen deraf. Inden en evt. ibrugtagning af ny teknologi, såsom Cloud-baserede systemer, skal der ligeledes gennemføres risikovurdering af denne.

Direktionen tager stilling til risikovurderingen og er ansvarlige for at udforme en sikkerhedsstrategi, der imødegår uacceptable risici under hensyntagen til de økonomiske forhold.

Klassifikation:
Alle data og informationer, hvor enkeltpersoner og/eller virksomheder er identificerbare, anses for værende fortrolige oplysninger. Ligeledes betragtes endnu ikke offentliggjort materiale (IOT) samt materiale af økonomisk, personalemæssig og strategisk art under udarbejdelse samt anden administrativ information som *fortrolige oplysninger*.
Fortroligheden sikres bl.a. via anvendelse af internationalt anerkendte metoder (eksempelvis anonymisering/pseudonymisering og kryptering).

Der henvises i øvrigt til datafortrolighedspolitikken for nærmere oplysninger og regler.

11 Informationssikkerhedsberedskab

Det følger af beredskabslovens paragraf 24, stk. 1, at ministrene har pligt til at sikre, at der gennemføres en forsvarlig beredskabsplanlægning inden for deres ressortområder. Som en del af forpligtelsen indgår afprøvning af beredskabet og gennemførelse af øvelser. Gennemførelse af øvelser bidrager til at styrke krisestyringsberedskabet og opbygge krisestyringsrutine i DST og kan være med til at afdække evt. svagheder i beredskabet. Øvelser er også vigtige for at teste, at organisationen, planerne og procedurerne virker efter hensigten.

Derfor skal DST have et it-beredskab som træder i kraft, når der sker informationssikkerhedsmæssige katastrofer og hændelser, såsom længerevarende nedbrud, strømsvigt, brand mv. It-beredskabet skal sikre, at der kan ske genetablering af systemerne, således at forretningsdriften kan fortsætte.

Som et element i at kunne genetablere DSTs systemer og sikre videre drift, skal DST sikre, at der kan ske ekstern nøddrift, hvilket vil sige, at de vigtigste systemer kan køre videre på et eksternt beliggende katastrofe-site. Dette dækker fx driften af hjemmeside, databanker og Lovmodellen samt datadelingsløsninger, selvom DSTs it-miljø i maskinstuen skulle være utilgængeligt.

DST skal endvidere sikre fortsat drift i en periode med strømsvigt ved at have nødstrømsanlæg, som kan holde DSTs it-miljø kørende i en periode.

12 Afvigelser og internt tilsyn

Afvigelser
Hvis der opstår situationer, hvor kravene i informationssikkerhedspolitikken ikke kan efterleves, skal der skriftligt anmodes om dispensation, stilet til Informationssikkerhedsudvalgets formand. Eventuelle afvigelser fra kravene skal dokumenteres, og der skal indføres alternative sikringsforanstaltninger.
Der tages dog højde for beredskabssituationer, hvor akutte kriser kan medføre midlertidige afvigelser, der må besluttes på stedet. Sådanne tilfælde skal efterfølgende anmeldes til Informationssikkerhedsudvalgets formand.

Internt tilsyn
Ifølge ISO 27001 og Danmarks Statistiks informationssikkerhedsstrategi er ansvaret for informationssikkerheden og dermed også for det interne tilsyn forankret hos ledelsen, herunder direktøren for Brugerservice. Der er udpeget en overordnet ansvarlig, der i sikkerhedsspørgsmål refererer til direktøren for Brugerservice, og som skal etablere og vedligeholde et samlet overblik over DST's interne tilsyn.

Det interne tilsyn skal sikre, at der sker udarbejdelse og vedligeholdelse af en overordnet plan for internt tilsyn med udgangspunkt i SoA-dokumentet. Desuden skal tilsynet sikre, at de interne tilsyn gennemføres med de angivne intervaller for hver SoA kontrol, at de dokumenteres og at der sker opfølgning på resultaterne af tilsynene. Tilsynene er baseret på stikprøvekontroller indenfor de aktuelle områder samt gennemgang og vurdering af de rapporter, der dannes på basis af den foretagne logning.

Endelig skal det sikres at der sker rapportering af resultaterne af de interne tilsyn til ledelsen og til Informationssikkerhedsudvalget ved de ordinære og evt. ekstraordinære møder.

Informationssikkerhedskoordinatoren er udpeget som ansvarlig for planlægning af det interne tilsyn.

Afvigelser, der konstateres i forbindelse med gennemførelse af det interne tilsyn, registreres og behandles i sammenhæng med den øvrige risikostyring.

13 Opfølgning

DST måler, vurderer og følger op på informationssikkerhedsområdet på følgende måde:

1. DST skal følge op på informationssikkerheden ved fortsat at optimere ledelsessystemet igennem løbende vedligehold og optimering af informationssikkerhedsstrategien, informationssikkerhedspolitikken og de dertilhørende regler og procedurer. Målet er, at sikre en struktureret og kontinuerlig forbedringsproces og ISO 27001 certificering på udvalgte områder.
2. Der gennemføres uafhængige tredjepartsrevisioner og tilsyn, der gennemføres af ressortområdets departement og af Rigsrevisionen.
3. Der foretages en årlig risikovurdering, hvor der efter behov inddrages uvildige eksterne konsulenter.
4. Der foretages en årlig sikkerhedstest af DSTs eksternt rettede systemer med henblik på at identificere eventuelle risici for systemindtrængning mv.
5. Løbende registrering og opfølgning på hændelser inden for informationssikkerhedsområdet.
6. Afdelingsdirektøren for Brugerservice og efterfølgende informationssikkerhedsudvalget orienteres om alle hændelser. Ved større nedbrud udarbejder IT en redegørelse til Direktionen vedr. konsekvenser, årsager og løsninger.

14 Vedligehold og ikrafttrædelse

Håndtering af ændringer i sikkerhedsdokumentationen foretages på følgende måde:

- Informationssikkerhedspolitikken: skal godkendes af Informationssikkerhedsudvalget og Direktionen. Politikken skal vedligeholdes med jævne mellemrum, hvilket som minimum er en gang om året.
- Informationssikkerhedshåndbogen inkl. relevante bilag og retningslinjer: skal godkendes af Informationssikkerhedsudvalget. Væsentlige procedurer skal gennemses og vedligeholdes med jævne mellemrum.
- Operationelle procedurer: skal vedligeholdes og godkendes af it-sikkerhedsgruppen.

Informationssikkerhedspolitikken er godkendt på Informationssikkerhedsudvalgets møde den 11. december 2019 samt af Direktionen den 11. marts 2020, hvorefter den er trådt i kraft.