DANMARKS STATISTIK

Danmarks Statistiks informationssikkerhedspolitik

Vi passer godt på data i en digital verden

Danmarks Statistik er den centrale statistikproducent i Danmark og har gennem mange år behandlet fortrolige data til brug for belysning af samfundsforholdene. Danmarks Statistik opererer på et sæt af kerneværdier, som er troværdighed, åbenhed, brugerfokus, forandringsevne og dataansvarlighed.

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 og mange udfordringer ift. datasikkerhed. I Danmarks Statistik foregår der et tilsvarende kontinuert arbejde med at udvikle de procedurer og sikringsmekanismer, som vi har sat op omkring vores mange data. Befolkningen og brugerne af vores tjenester skal fortsat kunne have tillid til, at data er i sikre hænder.

Danmarks Statistik 26. februar 2024

Birgitte Anker
Rigsstatistiker

Indhold

1 Indledning

Dette er Danmark Statistiks informationssikkerhedspolitik, som fastsætter rammerne for arbejdet med sikkerhed i Danmarks Statistik, og som følger informationssikkerhedsstandarden ISO27001:2022.

I øvrigt henvises til Digitaliserings- og Ligestillingsministeriets 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 Danmarks Statistiks behandling og kommunikation af information. Det er uanset om det er i elektronisk form eller i papirform, ligesom teknologi og organisatoriske processer også er omfattet.

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

- Danmarks Statistiks til enhver tid gældende strategi, pt. Strategi 2025
- Forskrifter, lovgivning/forordninger og direktiver mv. inden for Danmarks Statistiks område, herunder ISO 27001 samt Databeskyttelsesforordningen (GDPR)
- Det nuværende og forventede trusselsmiljø vedrørende informationssikkerhed.

Danmarks Statistik skal på baggrund af systematiske risikovurderinger og en konkret sandsynligheds-og konsekvensanalyse sikre det sikkerhedsniveau, som Danmarks Statistiks direktion har besluttet, og som svarer til værdien af informationsaktiverne i Danmarks Statistik.
Desuden har Danmarks Statistik 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 foranstaltninger, som er specifikke for Danmarks Statistik.

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 Danmarks Statistik.

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

Danmarks Statistiks informationssikkerhedspolitik beskriver vigtigheden af arbejdet med informationssikkerhed i organisationen og fastlægger ambitionsniveauet herfor. Informationssikkerhedspolitikken indeholder derfor de overordnede sikkerhedsmålsætninger og danner grundlag for udformning af Danmarks Statistiks informationssikkerhedshåndbog, der skal forstås som fællesbetegnelsen for informationssikkerhedspolitikken med de underliggende regelsæt og procedurer.

Danmarks Statistiks vigtigste dokumenter og politikker vedr. informationssikkerhed af ekstern interesse (inkl. nærværende informationssikkerhedspolitik) publiceres også på Danmarks Statistiks hjemmeside og befinder sig pt. på https://www.dst.dk/da/OmDS/datasikkerhed-i-danmarks-statistik/

2 Målsætningerne for informationssikkerhed i Danmarks Statistik

Det er Danmarks Statistiks 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 Danmarks Statistik, 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.

Der er tre store grundsten, som informationssikkerhed hviler på, og de drejer sig om datas fortrolighed, om datas integritet samt tilgængeligheden af data (i deres systemer). Fortrolighed skal forstås således, at information kun vises til de der har rettigheder til at se pågældende data. Integritet omfatter at data er korrekte og tilgængelighed betyder at data kan tilgås, altså at systemer er "oppe".

Danmarks Statistiks informationssikkerhedsmålsætninger tager udgangspunkt i fortrolighed, integritet og troværdighed, og er således:

1. at **fortrolige informationer, herunder alle ikke-offentliggjorte statistikdata, beskyttes** mod uautoriseret adgang.

    Det omfatter bl.a.:

    - fortrolig behandling, transmission og opbevaring af data, bl.a. ved brug af afidentificering/pseudonymisering og kryptering,
    - forhindring af identifikation af enkeltpersoner og enkeltmandsvirksomheder, bl.a. gennem afidentificering og diskretionering, som det er beskrevet i Danmarks Statistiks Datafortrolighedspolitik
    - forhindring af datatab og - lækager
    - understøttelse af overholdelsen af Databeskyttelsesforordningen (GDPR), også som databehandler for andre

2. at **alle informationer**, statistikdata såvel som ikke-statistikdata, **er korrekte og fuldstændige** og at it-systemer fungerer korrekt.

    Det omfatter bl.a:

    - automatiserede og manuelle kontrolforanstaltninger, der bl.a. skal forhindre svig og bedrag
    - sikring af korrekt funktion af it-systemerne med minimeret risiko for manipulation af data og systemer

3. at **alle informationer**, både statistikdata og ikke-statistikdata, og it-services er **tilgængelige**.

    Det omfatter bl.a.:

    - sikring af driftssikkerhed og minimering af risiko for større nedbrud, fx som følge af cyberterrorisme og angreb på infrastruktur.

Alle tre målsætninger understøttes af målrettet arbejde med 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.

Det skal i øvrigt bemærkes, at Danmarks Statistik ikke råder over systemer med personoplysninger, der af Justitsministeriet er defineret til alene at måtte opbevares i Danmark (lokationskravet i databeskyttelsesloven).

Danmarks Statistik 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. Dataansvarlighed er med andre ord en eksplicit nøgleværdi af strategisk karakter hos Danmarks Statistik, der også indgår som selvstændigt område i Strategi 2025.

Danmarks Statistik er blevet ISO 27001 certificeret første gang i 2020 med scopet statistikproduktionen, samt dertilhørende it-og forretningsprocesser som en dokumentation af et højt sikkerhedsniveau, og der bliver fulgt op på denne årligt af eksterne auditører. I 2023 blev Danmarks Statistik recertificeret og overgik samtidig til ISO 27001:2022.

Ligeledes får Danmarks Statistik løbende udstedt ISAE 3000 erklæringer som dokumentation for overholdelse af GDPR (Persondataforordningen).

3 Politikkens omfang

Informationssikkerhedspolitikkens scope og omfang defineres således:

- Informationssikkerhedspolitikken gælder for alle ansatte i Danmarks Statistik uanset ansættelsesform, herunder også eksterne konsulenter og servicemedarbejdere.
- Informationssikkerhedspolitikken gælder for alle systemer og alle data i Danmarks Statistiks besiddelse.
- Leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til Danmarks Statistiks 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 Danmarks Statistiks 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 Danmarks Statistik arbejder efter.

4 Overtrædelse af politikken

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

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

Sanktionerne kan være ansættelsesretlige, erstatningsretlige og/eller strafferetlige, afhængig af omstændighederne og situationen

Hvis en medarbejder er vidende om, at Danmarks Statistiks informationssikkerhed overtrædes, skal det meddeles til informationssikkerhedskoordinatoren, direktøren for Brugerservice eller Servicedesk hurtigst muligt.

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 direktionen. Informationssikkerhedskoordinatoren er ansvarlig for implementering og vedligeholdelse af informationssikkerhedssystemet i Danmarks Statistik 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.

Danmarks Statistik 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.

Danmarks Statistik 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 Danmarks Statistiks governancemodel på sikkerhedsområdet.

Danmarks Statistik har udpeget systemejere, som er de fagligt ansvarlige for Danmarks Statistiks systemer. Systemejerne er typisk cheferne i IT samt kontorchefer for statistikkontorerne. De skal sikre, at de gældende informationssikkerhedsregler overholdes for deres systemer. Ligeledes skal systemejerne sikre overholdelse af GDPR (Persondataforordningen) samt føre tilsyn med databehandlere.

6 Sikkerhedsbevisthed

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

Den nødvendige viden og kompetence omkring informationssikkerhed skal kommunikeres til alle medarbejdere, og der skal løbende arbejdes med holdninger, kultur og viden omkring informationssikkerhed. Dette skal ske i forbindelse med ansættelsen, ved intro-kurser samt løbende i form af jævnlige awareness-kampagner jf. det udarbejdede koncept for awareness på informationssikkerhedsområdet.

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

tildeling af individuelle adgangsrettigheder til fortrolige oplysninger i Danmarks Statistik. Datafor-trolighedspolitikken 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 Danmarks Statistik, findes tilgængelige på intranettet.

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 Danmarks Statistik informationssikkerhedshåndbog eller på anden vis understøtter ledelsessystemet for informationssikkerheden i Danmarks Statistik, herunder sikre at der foretages regelmæssig gennemgang og opdatering af dokumenterne.

9 Sikkerhedsniveau

Et tilstrækkeligt informationssikkerhedsniveau opnås igennem sikringsforanstaltninger, der sikrer:

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

   Fortrolighed: Danmarks Statistik skal løbende sikre, at indsamlede data bliver behandlet sikkert. Danmarks Statistik 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 Danmarks Statistik som strategisk mål at anvende afidentificerede data i størst muligt omfang.
   Integritet: Danmarks Statistik 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 Danmarks Statistiks dokumentation og test af systemerne er af høj kvalitet.
   Tilgængelighed: Danmarks Statistik arbejder løbende på at opnå en høj tilgængelighed med høje oppetider og minimeret risiko for nedbrud. Danmarks Statistik arbejder jf. Strategi 2025 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 Danmarks Statistiks it-aktiver, medarbejdernes kompetencer, organisationens image og informationer/data i Danmarks Statistiks varetægt.

For at fastholde det tilstrækkelige sikkerhedsniveau i Danmarks Statistik skal følgende overholdes:

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

10 Risikovurdering

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

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

Den forretningsmæssige risikovurdering
Informationssikkerheden i Danmarks Statistik skal tilgodese lov- og myndighedskrav, kontraktlige forpligtelser samt forpligtelser over for de aktører, der er forpligtigede til at anvende Danmarks Statistik. Det er Danmarks Statistiks målsætning at være bevidst om relevante risici, og forholde sig til disse set i lyset af Danmarks Statistiks økonomiske muligheder.

Der er fastlagt et koncept for gennemførelse af risikovurderinger og registrering af observationer. Risikovurderingerne forholder sig bl.a. GDPR-lovgivning, teknisk gæld, sikkerhedsbrud, sårbarheder, behov for logning, brug af ny teknologi og andre for det enkelte forretningsområde relevante problemstillinger

Der foretages årligt et antal risikovurderinger efter nærmere aftale med direktøren for Brugerservice fx via de samarbejdsfora hvor direktøren deltager. Det vil typisk være ved større ændringer i opgaver, leverandører, it-systemer eller anvendelsen deraf eller ved udefrakommende risici.

Ibrugtagning af ny teknologi
Hensynet til samfundet sættes højt, når Danmarks Statistik anvender ny teknologi, der skal finde anvendelse på fortrolige data og informationer, såvel i statistikproduktionen som ved administrationsdata.

Ikke mindst når og hvis der skal anvendes eksempelvis Cloud-baserede systemer, AI-løsninger eller løsninger, som indebærer brug af internetbaserede tjenester eller deling af oplysninger og data, skal der udarbejdes risikovurderinger. Sådanne løsninger ønsker Danmarks Statistiks ledelse, at der bliver taget eksplicit stilling til, og derfor skal der gennemføres risikovurderinger, konsekvensanalyser og lignende vurderinger, samt direktionsfremlæggelse inden ibrugtagning.

Ny teknologi kan forstås som teknologi og værktøjer, hvor statistikdata og andre fortrolige informationer behandles[1] i en nyligt udviklet og i Danmarks Statistik ikke

[1] Behandling som indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

tidligere anvendt applikation, metode, proces eller system. Eller hvor teknologien har potentiale til at transformere arbejdsformer, ændre adfærdsmønstre eller påvirke samfundet på forskellige måder.

Ved risikovurderinger af ny teknologi tages der stilling til hvordan den nye teknologi vil påvirke Danmarks Statistiks etablerede informationssikkerheds setup, ligesom konsekvenser for de brugere og virksomheder hvis data Danmarks Statistik anvender, skal overvejes. Dvs. at der foretages en vurdering af hvilke nye risici en teknologi kan introducere, og hvor der bør implementeres nye sikkerhedsforanstaltninger for at matche og sikre det eksisterende høje sikkerhedsniveau.

11 Dataklassifikation

Danmarks Statistik ligger inde med en stor mængde oplysninger om borgere og virksomheder, og mange af disse oplysninger har en fortrolig karakter. I henhold til lovgivningen i straffeloven og forvaltningsloven vil en bestemt del af de statistiske oplysninger i Danmarks Statistik være fortrolige. Danmarks Statistik har imidlertid valgt at klassificere alle statistikoplysninger som fortrolige for at sikre et ensartet højt niveau af fortrolighed.
Ligeledes betragtes endnu ikke offentliggjort materiale (IOT) samt eksempelvis materiale af personalemæssig art som *fortrolige oplysninger*.

Fortroligheden sikres bl.a. via anvendelse af internationalt anerkendte metoder i form af anonymisering/pseudonymisering og kryptering.

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

12 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 Danmarks Statistik 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 har Danmarks Statistik et it-beredskab, som træder i kraft, når der sker informations-sikkerhedsmæssige hændelser og katastrofer, 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 Danmarks Statistiks systemer og sikre fortsat drift, skal Danmarks Statistik sikre, at der kan ske ekstern nøddrift, hvilket vil sige, at de vigtigste systemer kan køre videre på et eksternt beliggende katastrofe-site.

Systemer indeholdt i nøddriften indstilles af Informationssikkerhedsudvalget, og forelægges efterfølgende direktionen.

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

13 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
Ansvaret for informationssikkerheden og dermed også for det interne tilsyn er forankret hos direktionen, herunder direktøren for Brugerservice.

Internt tilsyn gennemføres for at identificere, om der er en rød tråd igennem Danmarks Statistiks ISMS, gående fra risikobillede, topledelsens beslutninger og den overordnede informationssikkerhedspolitik, til de underliggende informations-sikkerhedspolitikker og procedurer, som skal opfylde informationssikkerhedskravene og til de implementerede kontroller.

Det interne tilsyn skal være uafhængigt, som beskrevet i konceptet for det interne tilsyn.

Det interne tilsyn består af udtagning af udvalg af stikprøver og indsamling af vidnesbyrd ved interview, ved gennemgang af projektdokumenter, ledelsessystemets dokumenter og tilhørende processer. Afvigelser, der konstateres i forbindelse med gennemførelse af det interne tilsyn, registreres og behandles i sammenhæng med den øvrige risikostyring.

Det interne tilsyn rapporterer til Informationssikkerhedsudvalget, som også beslutter hvem, der indgår i tilsynsteamet.

14 Opfølgning

Danmarks Statistik måler, vurderer og følger op på informationssikkerhedsområdet på følgende måde:

1. Danmarks Statistik 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 opretholdelse af 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 løbende risikovurdering, hvor der efter behov inddrages uvildige eksterne konsulenter.
4. Der foretages en årlig sikkerhedstest af Danmarks Statistiks 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.

15 Vedligehold og ikrafttrædelse

Håndtering af ændringer i sikkerhedsdokumentationen foretages på følgende måde:

- Informationssikkerhedspolitikken er godkendt af Informationssikkerhedsudvalget og direktionen. Politikken skal vedligeholdes med jævne mellemrum, hvilket som minimum er en gang om året.
- Informationssikkerhedshåndbogen inkl. relevante bilag og retningslinjer er godkendt af Informationssikkerhedsudvalget. Større ændringer godkendes af udvalget inden idriftsættelse
- Operationelle procedurer og mindre ændringer til informationssikkerhedshåndbogen vedligeholdes og godkendes af it-sikkerhedsgruppen.

Informationssikkerhedspolitikken er behandlet på Informationssikkerhedsudvalgets møde den 8. januar 2024, samt af direktionen den 26. februar 2024, hvorefter den er trådt i kraft.