

Kontor/afdeling
PR/RC

Dato
27. november 2025

J nr.

/ 2025-111

DMI's cyber-, informations- og informationssystemssikkerhedspolitik

Indledning

Denne cyber-, informations- og informationssystemssikkerhedspolitik er den overordnede ramme for informationssikkerheden hos Danmarks Meteorologiske Institut (DMI). Som et led i den overordnede informationssikkerhedsstyring tager øverste ledelse, på grundlag af den løbende overvågning og rapportering, informationssikkerhedspolitikken op til revurdering mindst én gang om året.

Cyber-, informations- og informationssystemssikkerhedspolitikken understøtter DMI's mission, vision og strategiske grundlag, idet DMI bygger sin forretning på et fundament af data, information og informationssystemer. Den sikrer fokus på robust forretningsdrift samt efterlevelse af love og regler på området. Styring af cyber- og informationssikkerheden er en central opgave for statslige myndigheder. DMI skal derfor efterleve NIS2-loven, der implementerer EU's Net- og Informationssikkerhedsdirektiv (NIS2), CER-loven, der implementerer EU's Critical Entities Resilience-direktiv (CER) samt den internationale standard for styring af informationssikkerhed ISO/IEC 27001. Derudover skal de tekniske minimumskrav for statslige myndigheder efterleves. Det skærpede trusselsbillede med stigende cybertrusler samt kravene i databeskyttelseslovgivningen og EU's databeskyttelsesforordning stiller yderligere krav til DMI's sikkerhedsniveau.

Definitioner

Ved

- data forstås en samling af oplysninger, tal, statistikker, billeder mv., som relaterer sig til et objekt, her DMI.
- informationer forstås data, der har gennemgået en behandling, således at de repræsenterer en større værdi for brugeren end de indgående data alene ville gøre.
- et informationssystem forstås ethvert manuelt eller automatisk system til fremstilling, lagring, behandling eller udbredelse af informationer.
- informationssikkerhed forstås ethvert sikkerhedsmæssigt aspekt, som vedrører data, informationer eller informationssystemer.

Referencer

ISO 27001:2022

NIS2-loven

CER-loven

De tekniske minimumskrav

Databeskyttelsesloven og databeskyttelsesforordningen

Formål

Formålet med cyber-, informations- og informationssystemssikkerhedspolitikken er at definere en ramme for beskyttelse af virksomhedens informationer og særligt at sikre, at kritiske og følsomme data, informationer og informationssystemer bevarer deres:

- fortrolighed, der skal sikre, at informationerne er beskyttet mod afsløring og uautoriseret anvendelse.
- integritet, der skal sikre, at informationerne er akkurate og fuldstændige og at de anvendte IT-systemer fungerer korrekt.
- tilgængelighed, der skal sikre, at informationerne, med tilhørende service, er tilgængelige på de tidspunkter, forretningsprocesserne fordrer det.
- autenticitet, der skal sikre informationernes ægthed, og at afsender er, hvad den foregiver at være.

Politikkens formål er endvidere at tilkendegive over for alle, som har en relation til DMI, at anvendelse af data, informationer og informationssystemer er underlagt passende standarder og retningslinjer. Målet er, at sikkerhedsproblemer forebygges, eventuelle skader begrænses og retablering af informationer kan sikres for herigennem at beskytte den vedvarende varetagelse af DMI's ansvar.

Formålet med politikken er samtidig at sikre informationer i samarbejder og aftaler med 3. part.

Informationssikkerhedsstandard ISO 27001:2022 er obligatorisk for statens institutioner. Sikkerhedsstandard stiller krav om, at der skal etableres et ISMS (Information Security Management System) i organisationen. ISMS er en samlet ramme for de politikker, procedurer, beslutningsgange og aktiviteter, som udgør komponenterne i organisationens arbejde med informationssikkerhedsstyring. Et ISMS er en metode til at styre sikkerhed, som kan gøre det nemmere at leve op til standarden.

Desuden skal DMI efterleve NIS2-loven, som implementerer EU's Net- og Informationsdirektiv. NIS2-direktivet skal sikre en styrkelse og harmonisering af cyber- og informationssikkerheden på tværs af EU's medlemslande. Direktivet stiller yderligere krav til forsyningskædesikkerhed, risikostyring, hændelsesunderretning til myndighederne inden for fastsatte tidsfrister samt ledelsens ansvar for cyber- og informationssikkerhed. Samtidig skal DMI efterleve CER-loven, der implementerer EU's direktiv om Critical Entities Resilience, der skal sikre modstandsdygtigheden i kritisk infrastruktur. NIS2 fokuserer på cybersikkerhed, mens CER fokuserer på modstandsdygtigheden mod en bredere vifte af trusler som naturkatastrofer og terrorangreb. De to direktiver supplerer dermed hinanden.

Omfang og ansvar

Informationssikkerhedspolitikken omfatter DMI's egne data og informationer, samt data og informationer, der ikke tilhører DMI, men som DMI kan gøres ansvarlig for. Dette

inkluderer f.eks. alle data om personale, data om finansielle forhold, alle data, som bidrager til administrationen af virksomheden, produktionsdata og anlægsdata samt informationer, som er overladt DMI af andre.

Denne politik omfatter alle ovennævnte data og informationer, ligegyldigt hvilken form de opbevares, behandles og formidles på.

Behandling af persondata skal desuden ske i henhold til KEFM's persondatapolitik og i henhold til databeskyttelsesloven og EU's databeskyttelsesforordning.

Denne politik gælder for alle ansatte uden undtagelse, både fastansatte personer og personer, som midlertidigt arbejder for DMI, inklusiv konsulenter der arbejder på vegne af DMI. Alle disse personer bliver her betragtet som "medarbejdere".

Ansvar for informationssikkerhedspolitikken er forankret hos DMI's øverste ledelse. Det operationelle ansvar er placeret hos DMI's informationssikkerhedsudvalg (ISU) jf. bilag 1. Den daglige styring af informationssikkerhedsindsatsen foretages af DMI's informationssikkerhedskoordinator, som refererer til instituttets informationssikkerhedsudvalg. Udvalget og informationssikkerhedskoordinatoren sikrer, at de aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger, der er beskrevet i DMI's informationssikkerhedsniveau gennemføres og efterleves. Herigennem skal hensynet til informationssikkerhed integreres i alle forretningsgange, driftsopgaver og projekter.

Leverandører og samarbejdspartnere

Ved udlicitering, herunder ved kongelig resolution, af arbejdsopgaver skal det sikres, at DMI's sikkerhedsniveau fastholdes. Dette sker ved, at serviceleverandøren, der har adgang til DMI's informationer, som minimum lever op til DMI's informationssikkerhedsniveau, herunder databeskyttelsesloven og EU's databeskyttelsesforordning (navnlig kravet om databehandlaftaler) samt DMI's procedure for leverandørstyring. Dette gælder også for underleverandører, hvilket er serviceleverandørens ansvar. For fællesstatslige løsninger ligger ansvaret for leverandørstyring hos Finansministeriet, ligesom Økonomistyrelsen har ansvaret for sikkerheden i de fællesoffentlige systemer, som styrelsen stiller til rådighed, og som DMI er forpligtet til at benytte.

Der skal indgås skriftlige aftaler med eksterne samarbejdspartnere og serviceleverandører, og de sikkerhedskrav, der stilles, skal fremgå af de skriftlige aftaler. For at sikre klarhed over de sikkerhedskrav, der stilles, skal der ske en konkret identifikation af risici i forbindelse med brug af eksterne leverandører. Serviceleverancer skal overvåges for at sikre, at den aftalte ydelse og de aftalte sikkerhedskrav overholdes.

Informationssikkerhedsniveau

Det er DMI's politik at beskytte sine informationer og udelukkende tillade brug, adgang og offentliggørelse af informationer i overensstemmelse med instituttets retningslinjer.

DMI's informationssikkerhedsniveau skal vedvarende være afstemt efter risiko og væsentlighed samt overholde lovkrav og indgåede aftaler, herunder licensbetingelser. DMI fastlægger sikkerhedsniveauet gennem en afbalanceret risiko- og konsekvensvurdering under hensyntagen til de økonomiske forhold. Cyber- og informationssikkerheden tilrettelægges således ud fra en risikobaseret tilgang, hvor væsentlige drifts- og sikkerhedshændelser forebygges, samtidig med at ressourceforbruget til sikkerhedsforanstaltninger afstemmes proportionalt i forhold til risikoen. Dette opnås gennem systematisk risikostyring og periodisk risikovurdering af DMI's informationsaktiver.

Der gennemføres mindst en gang årligt en risikovurdering. Der foretages ligeledes en risikovurdering ved større forandringer i organisationen eller proces-/systemporteføljen. DMI's informationssikkerhedsniveau bygger på ISO 27001:2022 samt kravene i NIS2 og CER tilpasset DMI's forretningsmål, risikovurdering og risikovillighed. Implementeringen koordineres med KEFM, så krav herfra ligeledes understøttes.

Målsætninger og metode til målbarhed

DMI udarbejder handleplaner for forbedringer i informationssikkerheden på baggrund af risikovurderinger og hændelser. Mål og metode afstemmes efter den konkrete sag. Derudover har DMI som målsætning at leve op til 'styret og målbart' i de årlige modenhedsmålinger vedr. implementeringen af ISO 27001. DMI bruger resultater fra tilsyn, fx halvårslige status på efterlevelse af de tekniske minimumskrav, årligt tilsyn med informationssikkerhed mm. som pejlemærker for arbejdet med informationssikkerhed. Der udarbejdes handleplaner på baggrund af tilsyn, som DMI løbende følger op på.

DMI's mål- og resultatplan indeholder også målsætninger ift. informationssikkerhed. Der følges op på målene i denne plan kvartalsvist.

Gennemgang af informationssikkerhedssystemets (ISMS) effektivitet og review

DMI vil årligt afprøve informationssikkerhedssystemets robusthed og effektivitet ved at foretage auditering af systemets effektivitet. I denne forbindelse inddrages resultat af risikoanalyse og beredskabsøvelser. Ekstern audit foretages af Rigsrevisionen.

Sikkerhedsbevidsthed

Informationssikkerhed vedrører DMI's samlede informationsstrøm, og implementeringen af en informationssikkerhedspolitik kan ikke gennemføres af ledelsen alene. Alle medarbejdere skal holdes orienteret om deres ansvar for at bidrage til at beskytte DMI's data og informationer mod hændelser og brud på informationssikkerheden. Alle medarbejdere skal derfor løbende uddannes i informationssikkerhed i relevant omfang.

Som brugere af DMI's informationer skal alle medarbejdere følge den til enhver tid gældende informationssikkerhedspolitik og de retningslinjer, der er afledt heraf.

Medarbejderne må kun anvende virksomhedens data og informationer efter arbejdsmæssigt behov og i overensstemmelse med informationernes følsomhed og/eller kritiske natur.

Beredskab

Beredskabet skal kunne aktiveres i tilfælde af, at der opstår utilsigtede hændelser, der i et vist omfang forstyrrer DMI's informationssikkerhedsaktiver eller samlede informationsstrøm.

Beredskabet koordineres af DMI's beredskabsteam og omfatter planer for krisestyring, planer for nøddrift af de mest kritiske opgaver og planer for reetablering af informationsstrømme. Planerne skal være opdaterede og tilgængelige på relevante steder.

Minimum en gang om året skal beredskabet øves og dokumenteres.

Brud på informationssikkerheden

Hvis en medarbejder bliver bekendt med trusler mod informationssikkerheden eller brud på denne, skal dette rapporteres ifølge gældende procedure for håndtering af hændelser. Dette gælder ligeledes forbedringsforslag og eventuelle observationer, der vedrører informationssikkerheden.

Hændelser, der opfylder kriterierne for anmeldelse til nationale tilsynsmyndigheder eller samarbejdspartnere i henhold til NIS2, skal rapporteres inden for de fastsatte tidsfrister. Formålet er at sikre hurtig reaktion, korrekt dokumentation, læring af hændelsen og forebyggelse af gentagelser, samtidig med at integritet, tilgængelighed, fortrolighed og autenticitet af informationer og informationssystemer opretholdes.

Medarbejdere, som forsætligt bryder informationssikkerhedspolitikken eller deraf afledte retningslinjer, kan blive udsat for disciplinære forholdsregler i overensstemmelse med DMI's gældende regler og personalepolitik.

DMI indsamler viden om informationssikkerhedshændelser i et system, som understøtter løbende behandling, logning og formidling af opnået viden og erfaring omkring eventuelle informationssikkerhedsbrud, nærhændelser og forbedringsforslag. Denne viden behandles og formidles via Informationssikkerhedsudvalget ud i organisationen, og ledelsen forpligter sig til, på denne baggrund, at inddrage denne viden i ressourceplanlægningen for DMI's videre udvikling af informationssikkerheden.

Godkendelse

Cyber-, informations- og informationssystemssikkerhedspolitikken for DMI godkendes af informationssikkerhedsudvalget (ISU) og revurderes mindst en gang årligt eller ved ændringer i risikobilledet, større organisatoriske ændringer eller opdatering af gældende lovgivning, herunder NIS2 og CER. Politikken kommunikeres ud til alle ansatte på intranettet samt til eksterne parter på DMI's hjemmeside. Politikken kan endvidere vedhæftes kontrakter, databehandleraftaler og andre relevante aftaledokumenter med eksterne parter.

København, november 2025

Direktør Marianne Thyrring