Informationssikkerhedspolitik

DSB

Telegade 2, 2630 Taastrup, CVR nr. 25050053

Ansvarlig: IT Sikkerhed

Godkendt af: Bestyrelsen **Dato**: 18.12.2025

1. Introduktion

DSB's samfundsopgave er at skabe mobilitet, der ikke belaster klimaet. Som udbyder af kollektiv transport har vi et ansvar for at sikre rejsen mod en bæredygtig drift af en digital, elektrisk flåde, kundevendte løsninger og en effektiv drift af DSB. Den løbende realisering af DSB's målsætninger forudsætter generelt en betydelig digitalisering i DSB. Samtidig nødvendiggør trusselsbilledet et konstant fokus på cyber- og informationssikkerhed.

Et tilstrækkeligt niveau af cyber- og informationssikkerhed medvirker til at sikre en stabil service for vores kunder og tillid til en bæredygtig, kollektiv transportform. DSB sætter kunden i fokus, når vi skaber mobilitet, udviser samfundsansvarlig adfærd og arbejder informationssikkert.

Vi skal sikre, at informationer er pålidelige og tilgængelige samt at de kan genskabes. Vi skal beskytte følsomme informationer, herunder personoplysninger om kunder og medarbejdere samt fortrolige informationer om DSB. Informationer må kun være tilgængelige for autoriserede personer med et arbejdsbetinget behov, og informationer skal være beskyttet mod cyberangreb.

Informationssikkerhedspolitikken understøtter DSB's overordnede formål *Plads til alle på rejsen mod det bæredygtige*.

2. Formål

Vores formål med informationssikkerhedspolitikken er løbende at:

"udvikle og sikre et tilstrækkeligt niveau for informationssikkerhed baseret på en afvejning af risici og omkostninger, hvor der aldrig gås på kompromis med passagersikkerheden".

Politikken gælder for alle ansatte i DSB-koncernen samt eksterne konsulenter, der har adgang til DSB's systemer og informationer. Politikken omfatter alle benyttede it-systemer, uanset om de er interne, eksterne, administrative eller knyttet til vores togdrift. Politikken omfatter både informationer i den fysiske verden (fx papir og tale) og informationer, der behandles digitalt.

3. Vores ambition og mål

Som leverandør af samfundskritisk infrastruktur arbejder DSB løbende med at styrke cyber- og informationssikkerheden. Det gør vi bl.a. ved at efterleve gældende lovgivning i Danmark og EU, herunder lovgivning for kritisk infrastruktur. Vi samarbejder med relevante myndigheder og sektorfora om informationssikkerhed og vi opretholder en certificering inden for informationssikkerhed. Vi udvikler systemer og infrastruktur samt medarbejderne, ledelsen og kulturen, så vi arbejder informationssikkert.

Vores målsætninger for informationssikkerhed er at:

- Opretholde et certificeret ledelsessystem for informationssikkerhed
- Øge medarbejdernes bevidsthed om informationssikkerhed
- Opdage, undersøge og forhindre trusler mod informationssikkerheden i DSB
- Opdage, registrere og reducere informationssikkerhedsrisici

- Styre informationssikkerhed gennem øget anvendelse af teknologi.

Målsætninger er godkendt af direktørkredsen. De er udmøntet i underliggende målinger, som løbende rapporteres til direktørkredsen og bestyrelsen. Målingerne kan advare om it-sikkerhedsforhold.

4. Sådan når vi vores mål

Direktørkredsen er i samarbejde med bestyrelsen øverste ansvarlige for cyber- og informationssikkerhed i DSB. Direktørkredsen har det overordnede ansvar for, at vores ledelsessystem for informationssikkerhed er effektivt og løbende udvikles.

IT Sikkerhed skal sikre rammerne for den praktiske implementering af cyber- og informationssikkerhed.

Ledere og medarbejdere i DSB er ansvarlige for at arbejde informationssikkert og for at efterleve informationssikkerhedspolitikken og underliggende retningslinjer.

For at udvikle og sikre et tilstrækkeligt niveau for informationssikkerhed arbejder vi ud fra følgende principper:

- Vi vedligeholder og forbedrer løbende vores ledelsessystem for informationssikkerhed for at styrke cyber- og informationssikkerheden. Vi arbejder ud fra anerkendte standarder og rammeværker.

- Vi overholder relevante krav om informationssikkerhed, herunder love, regler og kontraktmæssige forpligtelser.

- Vi stiller krav til leverandører og underleverandørers informationssikkerhed. Vi følger op på, at ydelser og informationssikkerhed efterlever vores krav. Vi kan outsource vores opgaver, men ikke vores ansvar.

- Vi sikrer løbende, at ledelsen og medarbejdere har tilstrækkelig forståelse for deres ansvar for og rolle i at arbejde informationssikkert og iagttage gældende lovgivning på området.

- Vi arbejder ud fra en risikobaseret tilgang til informationssikkerhed, hvor aktuelle og forventede risici og trusler afvejes i forhold til forretningens krav og ledelsens forventninger.

- Vi overvåger trusselsbilledet og tilpasser løbende vores tiltag, så vi sikrer, at informationer er pålidelige, tilgængelige og kan genskabes. Vi beskytter følsomme og fortrolige informationer, så de kun er tilgængelige for autoriserede personer.

- Vi integrerer og systemunderstøtter informationssikkerhed i eksisterende aktiviteter, processer og arkitektur.

4.1. Påvirkninger, risici og muligheder

IT Sikkerhed arbejder struktureret med at forebygge, opdage og afhjælpe cyber- og informationssikkerheds-risici og muligheder. Direktørkredsen fastlægger et accepteret niveau for risici. Risici rapporteres løbende til direktørkredsen og bestyrelsen sammen med påvirkninger i form af trusler og hændelser samt mulige forbedringer.

DSB's væsentligste risici er, at sikkerheden for vores passagerer påvirkes, og at vi må indstille togdriften. Vi prioriterer tiltag, som forebygger og afhjælper disse risici og sikrer det nødvendige beredskab.

5. Organisation, ansvar og godkendelse

Bestyrelsen i DSB er overordnet ansvarlig for at godkende politikken.

Politikken er udmøntet i underliggende retningslinjer for informationssikkerhed, som definerer roller og ansvar for de enkelte områder. Retningslinjerne godkendes af underdirektøren for IT. IT Sikkerhed skal opdatere informationssikkerhedspolitikken og underliggende retningslinjer samt gøre medarbejderne bekendte med disse. IT Sikkerhed vurderer, om dispensationer fra krav i underliggende retningslinjer kan godkendes.

Politikken revideres årligt og ved væsentlige ændringer.

Definition af informationssikkerhed

Sikre fortrolighed, integritet og tilgængelighed ved at beskytte informationer og informationssystemer mod cybertrusler, uautoriseret adgang, brug, offentliggørelse, afbrydelse, ændringer eller ødelæggelse.

6. Samspil med andre politikker og retningslinjer

- Politik for samfundsansvar
- Compliancepolitik
- Politik for beskyttelse af personoplysninger
- Politik for Data Governance og Dataetik
- AI-Politik
- Adfærdskodeks for informationssikkerhed - ansatte i DSB
- Adfærdskodeks for informationssikkerhed - eksterne konsulenter mfl.
- Information Security Manual