SL01 Banedanmarks Informationssikkerhedspolitik

Offentlig information

banedanmark

Indhold

1 Resumé

Dette dokument repræsenterer Banedanmarks informationssikkerhedspolitik og sætter en overordnet ramme for arbejdet med informationssikkerhed, målsætning og niveau på området, samt organisering og fordeling af ansvar og roller på tværs af hele Banedanmark.

1.1 Metadata

Dokumentejer	CIF
Målgruppe	Banedanmark ansatte og samarbejdspartnere
Sagsbehandler	CISO Morten Pedersen (MPDR)
Publicering af dokument	Baneinfo og bane.dk
Klassifikation	Offentlig information

1.1.1 Dokumenthistorik

Forfatter	Ver.	Emne	Godkender	Dato
BFSK	1.2	Godkendt	CIF	23. april 2021
XKACA	1.3	Tydeliggjort reference til BDK's råd om informationssikkerhed	Styregruppen	5. november 2021
XKACA	1.3	Godkendt	CIF (DIR)	11. november 2021
XTWLE/ XNAGO/X KACA	1.4	Review 2022: Rettelse af kontroller til sikkerhedsforanstaltninger. Tilføjet præcisering af forpligtelse til løbende forbedring af ISMS-dokumenter. Redundante tekstafsnit fjernet. Tilføjet afsnit om overordnet koordinering af beredskab.	CIF (DIR)	22. april 2022
CNRA	1.5	Review 2023: Review af dokument og mindre rettelser l over ansvar fjernet.	CISO (MPDR)	20-04-2023

1.1.2 Referencer:

1. SL04 Efterlevelseserklæring (SoA): Der beskriver og forankrer de informations-sikkerhedskrav (ISO-kontrolmål), Banedanmark vælger at implementere og efterleve.
2. SL05 Fortegnelse over samfundskritiske forretningsprocesser, systemer og infrastruktur: Der danner grundlag for Banedanmarks ISO 27001 implementering og certificering.
3. SL06 Trusselsvurdering: Der præsenterer væsentlige aktuelle trusler, herunder kapacitet og incitament, i forhold til Banedanmarks samfundskritiske services.

2 Indledning

Banedanmarks informationssikkerhedspolitik sætter rammen for arbejdet med informationssikkerhed, målsætning og niveau på området, samt organisering og fordeling af ansvar og roller på tværs af hele Banedanmark.

Informationssikkerhedspolitikken understøtter Banedanmarks strategiske initiativ "Et sikkert digitalt Banedanmark" og lever op til gældende lov- og myndighedskrav samt sikrer, at Banedanmark er en troværdig samarbejdspartner overfor andre myndigheder, leverandører og kunder.

Understøttet af Digitaliseringsstyrelsens vejledninger og NIS-direktivet har Banedanmarks direktion besluttet, at kravene til informationssikkerhed og persondatabeskyttelse, samt øvrig håndtering af forretningskritisk data, mest hensigtsmæssigt og effektivt imødekommes ved certificering og efterlevelse af informationssikkerhedsstandarden DS/ISO/IEC 27001.

Som udgangspunkt er alle krav til Informationssikkerhed beskrevet i Banedanmarks SoA[1] herefter benævnt som " SL04 Efterlevelseserklæring (SoA)" jf. 1.1.2. Referencer. Efterlevelseserklæringens krav skal på et risikobaseret grundlag implementeres og efterleves i forhold til " SL05 Fortegnelse over samfundskritiske forretningsprocesser, systemer og infrastruktur:" jf. 1.1.2. Referencer.

Informationssikkerhedspolitikken sætter ligeledes retning for etablering, implementering, vedligeholdelse samt forbedring af Banedanmarks ledelsessystem for informationssikkerhed (ISMS)[2]. Ledelsessystemet udvikles gennem regelmæssige risikostyringsprocesser, som giver ledelsen, ansatte, leverandører samt øvrige med en tilknytning til Banedanmark en bevidsthed om niveauet for informationssikkerhed.

2.1 Mål med informationssikkerhedspolitik

Målet for informationssikkerhedspolitikken er gennem forankring af ansvar og udvælgelse af nødvendige sikkerhedsforanstaltninger (informationssikkerheds-kontroller) at fastlægge, hvordan og på hvilket niveau Banedanmarks samfundskritiske forretningsprocesser, systemer og infrastruktur skal beskyttes i forhold til informationers fortrolighed, integritet og tilgængelighed. Dette for at aktuelle trusler, sårbarheder og hændelser forebygges samt eventuelle skader begrænses.

[1] Statement of Applicability (SoA) oversættes til Efterlevelseserklæring

[2] Et ISMS (Information Security Management System) er et ledelsessystem til styring af informationssikkerhed. Kravene til ledelsessystemet er beskrevet i ISO 27001

3 Organisering, ansvar og roller

3.1 Direktionen

Direktionen har det overordnede ansvar for informationssikkerheden i Banedanmark, herunder at informationssikkerhedspolitikken, samt bilag, anviser klare retningslinjer, et synligt engagement samt en præcis placering af roller og ansvar.

Direktionen har ligeledes ansvaret for, at informationssikkerhedspolitikken (SL01 Banedanmarks informationssikkerhedspolitik) kommunikeres til Banedanmarks ansatte og samarbejdspartnere.

Informationssikkerhedspolitikken skal godkendes årligt af direktionen.

Direktionen har etableret et forum for informationssikkerhed, hvor opgaven og ansvaret varetages. Direktionen deltager aktivt i Informationssikkerhedsforum (CIF).

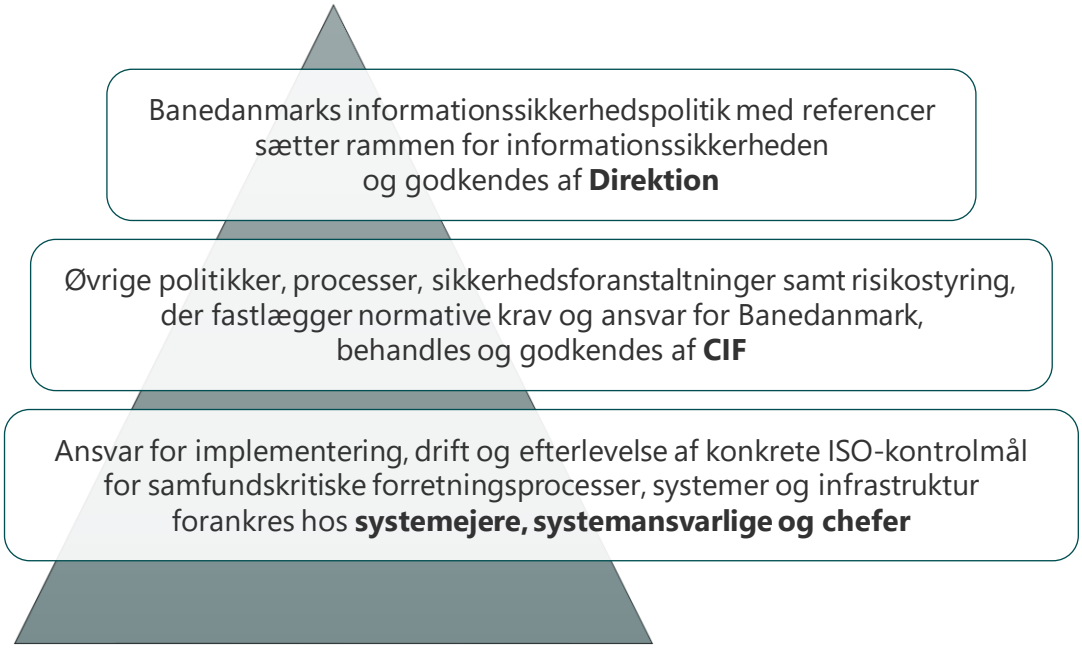
3.2 Informationssikkerhedsforum (CIF)

Økonomidirektøren (CFO) er formand for CIF. Den administrerende direktør er medlem af CIF. Der udpeges yderligere et medlem af direktionen til CIF.

Direktionen har delegeret den overordnede styring og koordinering af ledelsessystemet (ISMS) for informationssikkerhed i Banedanmark til Cyber- og informationssikkerhedsforum (CIF).

Formanden for CIF udpeger de øvrige medlemmer af CIF. Medlemskabet skal sikre sammenhæng og understøtte forankringen af cyber- og informationssikkerheds-arbejdet bredt og højt i Banedanmark, herunder koordinering med det øvrige sikkerhedsarbejde.

De overordnende aktiviteter for informationssikkerhed i form af fastlæggelse af det overordnede trusselsbillede, sikkerhedsniveau og risikobillede, implementering af sikkerhedsforanstaltninger, revisionsopfølgning, ledelsesrapportering samt kommunikation omkring politikker og retningslinjer er forankret i CIF.



CIF skal sikre, at informationssikkerheden er synlig og i overensstemmelse med Banedanmarks visioner og strategier samt løbende forbedres. Som udgangspunkt skal deltagerne være på direktør- eller områdechefniveau, men opgaver kan, med formandens godkendelse, uddelegeres.

3.3 Informationssikkerhedschef (CISO)

Banedanmarks Informationssikkerhedschef (CISO) har det daglige og operationelle ansvar for arbejdet med informationssikkerhed for hele Banedanmark samt varetagelsen af sekretariatsbistand til CIF. CISO har ligeledes ansvaret for den løbende udvikling, implementering, efterlevelse og opfølgning på informationssikkerhedsområdet.

CISO kan, på baggrund af identificerede risici, udforme retningslinjer, der fastsætter normative krav og ansvar inden for enkeltområder, herunder i forhold til implementering og efterlevelse af DS/ISO/IEC 27001. Alle krav, som berører organisatoriske områder og medarbejdere bredt i Banedanmark, skal godkendes i CIF.

3.4 Cyber- og informationssikkerhedssektionen (CIS)

Cyber- og informationssikkerhedssektionen ledes af Banedanmarks CISO og har ansvaret for, at informationssikkerheden i hele Banedanmark beskrives og kommunikeres, herunder at systemejere og -ansvarlige, chefer samt centrale leverandører, hvor muligt, er bekendt med Banedanmarks informationssikkerhedskrav og sikrer efterlevelse af disse.

Cyber- og informationssikkerhedssektionen er ligeledes ansvarlig for at rådgive, facilitere risiko- og sårbarhedsvurderinger og dispensationer samt bidrage til, at besluttede informationssikkerhedskrav efterleves på tværs af hele Banedanmark.

3.5 Chefer, systemejere og -ansvarlige

Chefer, systemejere og -ansvarlige er risikoejere indenfor eget ansvarsområde og bærer dermed ansvaret for, at Banedanmarks besluttede sikkerhedsforanstaltninger er implementerede og efterleves på baggrund af Cyber- og informationssikkerheds-forums anvisninger.

3.6 Ansatte og samarbejdspartnere

Informationssikkerhedsopgaven i Banedanmark kan ikke varetages af Banedanmarks ledelse alene. Alle medarbejdere og samarbejdspartnere har ansvar for at bidrage til at beskytte Banedanmarks informationer og aktiver mod uautoriseret adgang, ændring og ødelæggelse.

Alle ansatte i Banedanmark og samarbejdspartnere er forpligtet til at efterleve den til enhver tid gældende informationssikkerhedspolitik (SL01 Banedanmarks informationssikkerhedspolitik) samt tilhørende regler, retningslinjer, procedurer og relaterede bilag. Alle er forpligtet til at indberette sårbarheder eller sikkerhedshændelser til Banedanmarks servicedesk.

Konkret skal alle nyansatte ved deres tiltrædelse gøres bekendt med Banedanmarks informationssikkerhedskrav. Desuden skal alle i Banedanmark være vidende om, at de er underlagt tavshedspligt om fortrolige oplysninger, som de via deres arbejde får kendskab til.

Med henblik på at sikre en hensigtsmæssig og effektiv formidling uddrages de dele af informationssikkerhedspolitikken (SL01 Banedanmarks informationssikkerhedspolitik), regler og retningslinjer m.v. som er særligt relevante for medarbejdere og kontrahenter i Banedanmark, samt medarbejdere hos leverandører, i Banedanmarks råd om informationssikkerhed. Endvidere er de medarbejderrettede politikker indarbejdet i Medarbejderhåndbogen.

3.6.1 Overtrædelse af informationssikkerhedspolitikken

Overtrædelse af Banedanmarks sikkerhedsbestemmelser kan, efter omstændighederne, medføre sanktioner, hvilket fremgår af Medarbejderhåndbogen.

4 Beredskab

Banedanmarks beredskab skal sikre robusthed over for følgerne af fejlbehandling, ulykker og katastrofer og samtidig forhindre, at skader på personer, omdømme, ejendom og miljø mv. opstår.

Banedanmarks beredskab koordineres på overordnet niveau af Kvalitet & Sikkerhed, som også varetager al overordnet krisestyring.

Det er forretningsområdernes eget ansvar, at beredskabet er forankret, veltilrettelagt, internt koordineret og drevet af tilstrækkelige administrative, logiske og fysiske sikringsforanstaltninger. Banedanmarks beredskabsplaner skal ajourføres og testes løbende, og resultatet skal indgå i forretningsområdernes ledelsesrapportering.

Det er ligeledes forretningsområdernes eget ansvar at udarbejde og vedligeholde egne planer og processer for forretningskontinuitet på baggrund af aktuelle risikovurderinger.

5 Tilsyn og revision

Banedanmark fører tilsyn med og har intern revision af ISO 27001 standardens implementering og efterlevelse.

Det er forretningsområdernes og systemejers ansvar at sikre nødvendig revisionsopfølgning på baggrund af både intern og ekstern revision.

Banedanmarks tilsyn med 3. partsleverandører udøves i forbindelse med kontraktindgåelse, databehandleraftaler samt evt. kontrol af leverandørers revisionserklæringer m.v.

Trafikstyrelsen godkender Banedanmarks valg af et uafhængigt certificeringsorgan, som auditerer ISO 27001 standardens efterlevelse.

Rigsrevisionen reviderer Banedanmark på baggrund af aktuel lovgivning, herunder bl.a. efterlevelse af GDPR på ad hoc basis.