SL01 Banedanmarks Informationssikkerhedspolitik

Offentlig information

BANEDANMARK

Indhold

1 Resumé

Banedanmarks Informationssikkerhedspolitik er et helt grundlæggende dokument i Banedanmarks ledelsessystem for informationssikkerhed (ISMS), da det definerer Banedanmarks tilgang til informationssikkerhed. Det omfatter betydning af informationssikkerhed i relation til Banedanmarks formål, mål for informationssikkerheden, principper for informationssikkerhed, efterlevelsesmæssige forpligtelser, definition af ledelsesmæssig ramme, samt en forpligtelse til kontinuerlig forbedring af informationssikkerheden.

Dokumentets formål er at give retning og rammer for alle informationssikkerhedsrelaterede aktiviteter.

1.1 Metadata

Oversigt over metadata for dette dokument	
Dokumentejer	CIF
Målgruppe	Alle
Sagsbehandler	CIS
Publicering af dokument	Baneinfo og banedanmark.dk
Klassifikation	Offentlig information

Tabel 1.1 - Metadata

1.2 Dokumenthistorik

Forfatter	Version	Emne	Godkender	Dato
XTWLE	2.0	Dokument godkendt til udgivelse	CIF	4. juni 2024

Tabel 1.2 - Dokumenthistorik

Overordnet revisionshistorik for dette dokument.

1.3 Referencer

Dette dokument bygger på informationer fra følgende dokumenter:

- SL02 Omfang for ledelsessystem
- DS/EN ISO/IEC 27001:2023 Information - Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse - Ledelsessystemer for informationssikkerhed - Krav

2 Indledning

Dette dokument fastlægger den overordnede ramme for informationssikkerheden i Banedanmark, samt for etablering, drift og vedligeholdelse af et ledelsessystem for informationssikkerhed i overensstemmelse med ISO 27001:2023.

Banedanmarks Informationssikkerhedspolitik understøttes tillige af en række ledelsesdokumenter, emnespecifikke politikker, processer m.m.[1]

2.1 Godkendelse

Denne informationssikkerhedspolitik er gennemgået og kommenteret af alle medlemmer af Banedanmarks Cyber- og Informationssikkerhedsforum (CIF) og herefter tilrettet iht. indkomne kommentarer.

Banedanmarks Informationssikkerhedspolitik, er endeligt godkendt af CIF[2] på et ordinært CIF-møde, første gang den 11. marts 2024 og efterfølgende iht. årshjulet for informationssikkerhed[3].

2.2 Udgivelse og distribution

Banedanmarks Informationssikkerhedspolitik er klassificeret som offentlig information og er tilgængeligt på baneinfo (Banedanmarks intranet):

Cyber- og Informationssikkerhed > Banedanmarks ISMS >Styring og strategi

Derudover er Banedanmarks Informationssikkerhedspolitik også publiceret på Banedanmarks hjemmeside, Banedanmark.dk, hvor det er tilgængeligt for alle:

Leverandør > Normer, krav og regler > Politikker > Informationssikkerhedspolitik

Banedanmarks Informationssikkerhedspolitik kan derfor frit distribueres internt og eksternt til fx leverandører og ifm. udbud, og hvor dette måtte findes relevant i øvrigt.

2.3 Kontaktpunkt

Forespørgsler, forbedringsforslag og kritikpunkter til Banedanmarks Informationssikkerhedspolitik er altid velkomne. Alle henvendelser af denne art bedes rettet til Banedanmarks Chief Information Security Officer (CISO) på email-adressen informationssikkerhed@bane.dk.

---

[1] Jf. SL09 Dokumentation af Banedanmarks ISMS

[2] Cyber- og Informationssikkerhedsforum (CIF) er et ledelsesudvalg, udstyret med nødvendig autoritet til at lede og fordele arbejdet med informationssikkerhed i Banedanmark.

[3] Se PP01 Årshjul for Banedanmarks ISMS

3 Formål

Banedanmarks Informationssikkerhedspolitik er det overordnede udgangspunkt for at definere og kommunikere Banedanmarks forpligtelse til at beskytte data og informationssystemer, ikke kun internt, men også i relation til leverandører og forretningspartnere. Informationssikkerhedspolitikken etablerer de grundlæggende principper og retningslinjer, som sikrer fortrolighed, integritet og tilgængelighed af informationsaktiver.

Banedanmarks Informationssikkerhedspolitik fungerer som en paraply for mere detaljerede styrings- og ledelsesdokumenter og politikker, der dækker specifikke områder af informationssikkerhed.

Politikken skaber en ramme for viden, bevidsthed og ansvarlig adfærd i forbindelse med informationssikkerhed, både internt og i samarbejdet med eksterne parter, og understøtter organisationens overholdelse af relevante lovmæssige og regulatoriske krav, herunder etablering, drift og forbedring af Banedanmarks ledelsessystem for informationssikkerhed (ISMS) i overensstemmelse med ISO 27001:2023.

Banedanmarks Informationssikkerhedspolitik er en central del af Banedanmarks overordnede risikostyringsstrategi og understreger ledelsens engagement i at beskytte kritiske informationsaktiver og infrastruktur.

3.1 Ledelsens engagement

Banedanmarks direktion og øverste ledelse er fuldt forpligtede til at opretholde et højt niveau af informationssikkerhed og til at implementere, vedligeholde og kontinuerligt forbedre Banedanmarks ISMS i overensstemmelse med kravene i ISO 27001:2023.

Vi anerkender vigtigheden af at beskytte vores informationer og aktiver mod alle former for trusler, og træffer proaktive beslutninger for hele tiden at sikre fortroligheden, integriteten og tilgængeligheden af vores organisations, vores kunders og vores samarbejdspartneres informationer.

For at realisere denne forpligtelse vil vi sikre, at:

- ***Ressourcer er tilgængelige**: De nødvendige menneskelige, teknologiske og finansielle ressourcer allokeres for at implementere og vedligeholde Banedanmarks ISMS effektivt.*
- ***Risikostyring**: Vi systematisk identificerer, vurderer og håndterer informationssikkerhedsrisici i overensstemmelse med vores risikovurderings- og risikohåndteringsprocesser[4].*
- ***Overholdelse af lovgivning**: Vi forpligter os til at overholde alle relevante juridiske, lovmæssige, regulatoriske og kontraktlige forpligtelser.*

[4] SL07 Risikostyring og PP07 Proces for risikostyring

- ***Uddannelse og bevidstgørelse**: Alle medarbejdere og relevante eksterne parter uddannes og gøres bevidste om deres roller og ansvar i forhold til informationssikkerhed.*
- ***Kontinuerlig forbedring**: Vi forpligter os til kontinuerlig forbedring af vores ISMS gennem regelmæssig evaluering og revision.*

Denne politik understøtter Banedanmarks overordnede forretningsmål og sikrer, at informationssikkerhed forbliver en integreret del af vores forretningsprocesser.

Som Banedanmarks øverste ledelse vil vi regelmæssigt gennemgå denne politik og Banedanmarks ISMS for at sikre, at begge forbliver passende og effektive i forhold til vores organisations skiftende behov og omgivelser.

København, maj 2024

<Pladsholder - Signatur>

Hakon Iversen, Adm. Direktør

3.2 Anvendelsesområde og dækning

Banedanmarks Informationssikkerhedspolitik omfatter alle informationer i Banedanmarks besiddelse, både Banedanmarks egne informationer, samt alle informationer fra Banedanmarks interessenter, som Banedanmark kan stilles til ansvar for. Dette gælder uanset om der er tale om modtagelse, behandling, opbevaring eller afsendelse af informationer, og uanset om informationer håndteres analogt (fx papir, tale, viden eller fysiske aktiver) eller digitalt (fx i IT-systemer, digitale lagringsmidler, digital kommunikation eller multimedier).

- *Banedanmarks Informationssikkerhedspolitik gælder for alle ansatte i Banedanmark uanset ansættelsesform, herunder også eksterne konsulenter og servicemedarbejdere.*
- *Leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til Banedanmarks systemer og data, skal ligeledes have kendskab til og følge informationssikkerhedspolitikken, når de arbejder i Banedanmark regi.*
- *Informationssikkerhedspolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af Banedanmarks It-systemer, data og papirarkiver.*
- *Informationssikkerhedspolitikken gælder for alle informations- og kommunikationsteknologiske systemer i Banedanmark.*

Derimod er det jf. nedenstående afsnit ikke alle informations- og kommunikationsteknologiske systemer i Banedanmark, der er underlagt Banedanmarks ISMS.

3.2.1 Risikobaseret implementering

Banedanmarks øverste ledelsesorgan for informationssikkerhed, Cyber- og Informationssikkerhedsforum (CIF), har besluttet, at Banedanmarks ISMS implementeres progressivt, ud fra en risikobaseret betragtning, på alle kritiske informationsaktiver i Banedanmark, startende med Informationsaktiver/systemer/infrastrukturer, der kategoriseres som samfundskritiske[5], efterfulgt af de informationsaktiver/systemer/infrastrukturer, der kategoriseres som forretningskritiske.

Banedanmarks ISMS vil som udgangspunkt ikke blive implementeret på systemer, som ikke vurderes kritiske, men disse systemer vil stadig skulle leve op til Banedanmarks Informationssikkerhedspolitik, samt underliggende politikker, standarder og retningslinjer.

Ligeledes vil der være en række ældre legacy-systemer og andre systemer, hvor det af forskellige årsager ikke er muligt at sikre implementeringen af det fulde ISMS. Her vil der med udgangspunkt i risikovurderingen af systemet, blive implementeret de risikomitigerende tiltag, som ledelsen vurderer nødvendige.

En progressiv udrulning af ledelsessystemet medvirker til, at der både er tid og ressourcer til at sikre en bedre forståelse og forankring af ledelsessystemet, der hvor det rulles ud, samt at Banedanmark opnår en bedre og mere realistisk udnyttelse af de fagligt kompetente ressourcer, der er til rådighed, samt en mere skånsom udrulning uden risiko for at kompromittere driften af Banedanmarks kritiske forretningsprocesser.

En opdateret liste over informationsaktiver/systemer/infrastrukturer, der er blevet underlagt Banedanmarks ISMS, fremgår af styringsdokumentet SL05 Fortegnelse over kritiske informationsaktiver.

3.2.2 Certificering iht. ISO 27001:2023

Banedanmark er lovmæssigt forpligtet[6] til at få sit ledelsessystem for informationssikkerhed certificeret iht. ISO 27001 eller tilsvarende. Banedanmark har valgt at blive certificeret iht. ISO 27001:2023 (tidligere ISO 27001:2013)[7].

Jf. bekendtgørelsens[6] §5, stk. 5, gælder at "*Den akkrediterede certificering skal omfatte den del af operatørens net- og informationssystemer, som operatøren er afhængig af for at levere den væsentlige transporttjeneste, og hvor en hændelse vil få væsentlig forstyrrende virkning for leveringen af den pågældende transporttjeneste.*"

CIF har i overensstemmelse med ovenstående valgt, at certificeringen af Banedanmarks ISMS iht. ISO 27001:2023, kun skal gælde for informationsaktiver/systemer/infrastrukturer, der er kategoriseret som værende samfundskritiske.

---

[5] Se SL05 Fortegnelse over kritiske informationsaktiver

[6] Jf. BEK nr 1042 af 06/08/2018 - Bekendtgørelse om sikkerhed i net- og informationssystemer i transportsektoren, kapitel 3, §5.

[7] Se afsnit 4.5 for mere information.

En opdateret liste over informationsaktiver/systemer/infrastrukturer, der er vurderet som samfundskritiske, fremgår af styringsdokumentet SL05 Fortegnelse over kritiske informationsaktiver.

3.3 Brud på informationssikkerheden

Alle medarbejdere er personligt ansvarlige for at overholde Banedanmarks regler for informationssikkerhed og skriver under herpå ved ansættelsen.

Alle medarbejdere i Banedanmark, herunder også eksterne konsulenter, er forpligtede til, under udførelse af deres hverv, at efterleve den til enhver tid gældende informationssikkerhedspolitik med tilhørende politikker, retningslinjer, processer og relaterede bilag. En overtrædelse kan medføre sanktioner.

En overtrædelse af regler og anvisninger på informationssikkerhedsområdet kan efter en individuel og konkret vurdering få konsekvenser for den overtrædendes ansættelsesforhold i Banedanmark. Konsekvensen kan være, at denne meddeles en ansættelsesretlig sanktion i form af en påtale, advarsel, afskedigelse eller bortvisning.

Hvis en medarbejder er vidende om, at Banedanmarks Informationssikkerhedspolitik overtrædes, skal dette håndteres iht. afsnit 7.1 nedenfor.

4 Informationssikkerhed i Banedanmark

I en verden, hvor mængden af data vokser eksponentielt, og digitaliseringen dybt integreres i alle aspekter af det moderne liv, er informationssikkerhed blevet en kritisk komponent for organisationer af enhver størrelse.

Det samme gør sig gældende for Banedanmark, hvor det lidt atypisk ikke umiddelbart er mængden af data, der vokser eksponentielt. I Banedanmark er det primært digitaliseringen af togdriften og forretningsprocesserne, der driver behovet for informationssikkerhed. Hvad enten der er tale om signalsystemer, køreplanssystemer, informationssystemer, dataanalyse vha. machine learning eller koncernstyringssystemer som fx SAP, så vil de alle efterlade Banedanmark i en helt ny global sårbarhed, hvis ikke Banedanmark sikrer systemernes tilgængelighed, integritet og fortrolighed.

Informationssikkerhed implementeres gennem et sæt af politikker, processer, procedurer, administrative og tekniske foranstaltninger, softwareværktøjer og fysiske sikkerhedsforanstaltninger. Dette kan fx inkludere kryptering, adgangskontrol, netværkssikkerhed, antivirusprogrammer og sikkerhedsuddannelse for medarbejdere.

Det handler ikke kun om at beskytte informationsaktiver mod eksterne trusler som hackere og cyberangreb, men også mod interne trusler som utilsigtet datatab eller misbrug af information.

Informationssikkerhed understøtter tillige overholdelse af lovgivningsmæssige krav, beskytter Banedanmarks omdømme og sikrer fortsat tillid fra kunder og partnere.

4.1 Overordnede mål for informationssikkerhed

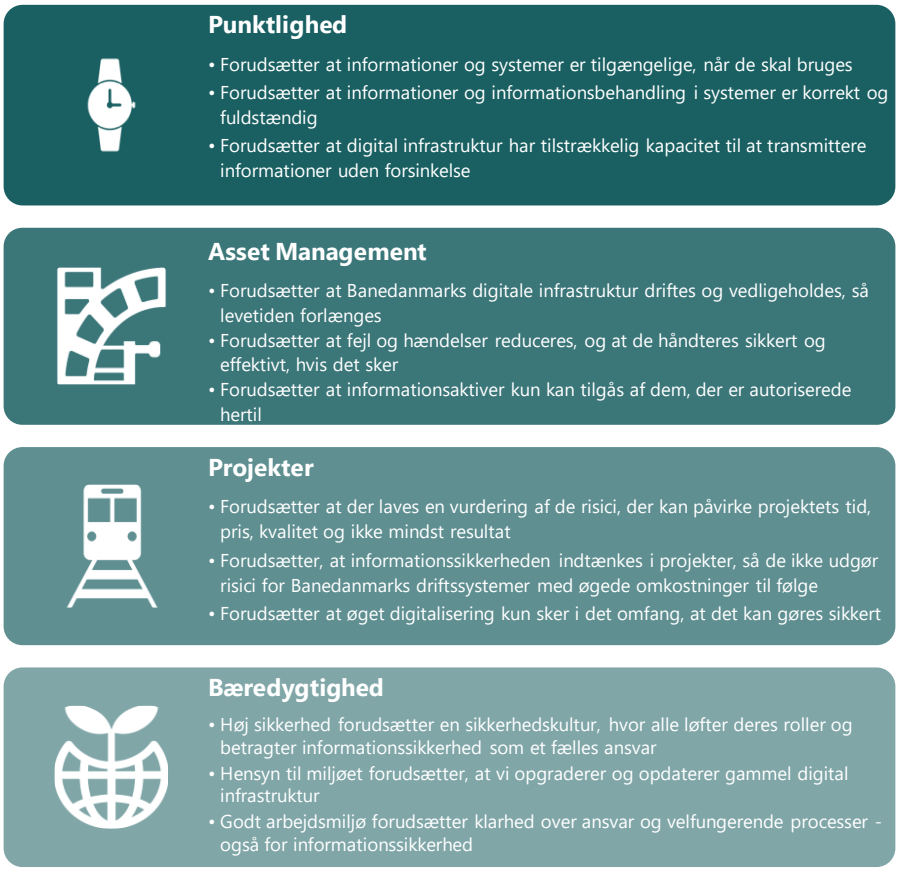
NIS-loven definerer sikkerhed som "*evnen for net- og informationssystemer til på et givet sikkerhedsniveau at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer*".

Overordnet set er Banedanmarks mål med informationssikkerhedsarbejdet derfor først og fremmest at sikre:

Tilgængelighed	Integritet	Autenticitet	Fortrolighed
• *Banedanmark vil sikre, at informationer med tilhørende IT-systemer og faciliteter er tilgængelige som aftalt og forventet.*	• *Banedanmark vil sikre, at informationer er fuldstændige, nøjagtige og reproducerbare, og at anvendte IT-systemer fungerer korrekt.*	• *Banedanmark vil sikre, at informationer er ægte og dermed, at der kan være tillid til gyldigheden af informationen, et signal eller en afsender.*	• *Banedanmark vil sikre, at informationer beskyttes mod afsløring, samt uautoriseret adgang og anvendelse.*

Banedanmarks fremtidige vision er at udvikle og bygge en attraktiv, grøn, sikker og effektiv jernbane. En vision der bliver kun til virkelighed, hvis vi i Banedanmark samarbejder effektivt om vores kerneleverancer; Punktlighed, Asset Management, Projekter og Bæredygtighed.

Som det fremgår af Figur 1 nedenfor, så er bl.a. informationssikkerhed en væsentlig forudsætning for at kunne levere på de fire ovennævnte kerneleverancer[8].



Figur 1. Informationssikkerhed i Banedanmarks kerneleverancer.

Banedanmarks informationssikkerhedspolitik har derfor også til formål at understøtte fremtiden ved at sikre, at Banedanmarks forretningsprocesser, herunder informationer, IT-systemer, infrastruktur, medarbejdere, opfylder de ovenfor angivne forudsætninger for de fire kerneleverancer.

[8] Jf. Banedanmarks strategi, " På vej mod fremtidens attraktive, grønne jernbane", Februar 2024.

For at sikre, at Banedanmarks indsats på informationssikkerhedsområdet udvikler sig i en retning, der kontinuerligt understøtter Banedanmarks strategi for fremtidens jernbane og evt. øvrige forretningsstrategier, så beslutter CIF hvert år en række klare, retningsspecifikke mål, der skal opnås gennem en række strategiske indsatser, samt overvåges og måles gennem nogle specifikke målepunkter.

Yderligere information om Banedanmarks kortsigtede og retningsspecifikke mål findes i:

- *SL03 Strategi og målsætninger for informationssikkerhed.*

4.2 Fundament for informationssikkerhed

Fundamentet for informationssikkerhed i Banedanmark defineres af en række grundlæggende principper. Disse principper definerer de afgørende rammer, der styrer beslutningstagning, strategiudvikling og daglig praksis i ledelsessystemets design, drift og evaluering. Udover at anvise rammer, så repræsenterer de grundlæggende principper også de kerneværdier og overbevisninger, som Banedanmarks ISMS er bygget på.

- *Grundlæggende principper danner fundamentet for, hvordan Banedanmark tilgår sikring af informationer og forretningsprocesser. De er vitale, fordi de sikrer en konsistent og effektiv tilgang til håndtering af informationssikkerhedsrisici.*
- *De hjælper med at etablere en fælles forståelse af, hvad der betragtes som vigtigt og nødvendigt for informationssikkerhed inden for Banedanmark.*
- *De understøtter udviklingen af politikker, procedurer og kontrolmekanismer, der er i overensstemmelse med Banedanmarks overordnede mål og risikotolerance.*
- *Grundlæggende principper er desuden vejledende for uddannelse og bevidstgørelse af medarbejdere og sikrer, at alle medarbejdere i Banedanmark arbejder mod fælles mål for informationssikkerhed.*

Overordnet set er de grundlæggende principper afgørende for at skabe en robust, holistisk og tilpasningsdygtig tilgang til informationssikkerhed, der kan modstå skiftende trusler og teknologiske udviklinger.

4.3 Grundlæggende informationssikkerhedsprincipper i Banedanmark

Banedanmarks ISMS bygger på nedenstående grundlæggende principper.

Princip	Forklaring
Tilgængelighed	Sikrer, at informationsaktiverne (data og informationssystemer) er tilgængelige og anvendelige ved anmodning fra en autoriseret entitet (bruger, system, proces).

Integritet	Sikrer nøjagtigheden og fuldstændigheden af data. Dette princip forhindrer uautoriseret ændring af information, sikrer, at data er pålidelige og korrekte, og garanterer, at ændringer kan spores.
Fortrolighed	Sikrer, at information kun er tilgængelig for dem med autoriseret adgang. Dette princip forhindrer uautoriseret afsløring af information og beskytter følsomme data mod eksterne eller interne trusler.
Autenticitet	Garanterer, at information, transaktioner og kommunikation er ægte. Dette princip omfatter identifikation og validering af brugernes identitet for at forhindre bedrageri og misbrug.
Uafviselighed	Sikrer, at handlinger eller transaktioner ikke kan nægtes senere. Dette opnås fx gennem logning, digitale signaturer og sporbarhed, hvilket sikrer ansvarlighed.
Risikostyring	Omfatter identifikation, vurdering og styring af risici for at minimere potentialet for sikkerhedshændelser. Dette princip er grundlaget for at træffe informerede beslutninger om sikkerhedsinvesteringer og kontrolforanstaltninger.
Minimumsrettigheder - "Principle of least privilege" (PoLP)	Begrænser brugeradgang til det niveau, der er nødvendigt for at brugere kan udføre deres arbejde. Dette reducerer risikoen for uautoriseret adgang til følsomme oplysninger.
Funktionsadskillelse	Opdeler kritiske funktioner og roller blandt flere personer eller grupper for at forhindre misbrug af autoritet og sikre, at ingen enkelt person kan kompromittere et system.
Gennemsigtighed og compliance	Sikrer, at sikkerhedstiltag er i overensstemmelse med lovgivningsmæssige og regulatoriske krav, og at de er gennemsigtige for relevante interessenter.
Kontinuerlig forbedring	Anvender en iterativ tilgang til at forbedre sikkerhedsprocesser og -foranstaltninger. Dette involverer regelmæssig evaluering og opdatering af sikkerhedstiltag for at imødekomme nye trusler og teknologiske ændringer.
Proaktivitet	Forudser og forbereder sig på nye og fremvoksende trusler ved at holde sig ajour med de seneste sikkerhedstendenser og trusselslandskaber. Dette princip indebærer forebyggende handlinger såsom regelmæssige sikkerhedsaudits og penetrationstests.
Holistisk tilgang	Integrerer informationssikkerhed i alle aspekter af Banedanmarks processer og kultur. Det sikrer, at sikkerhedsforanstaltninger er integreret i både tekniske og ikke-tekniske processer.
Alert awareness	Uddanner brugerne i god sikkerhedspraksis og opbygger en kultur af sikkerhedsbevidsthed og årvågenhed for at styrke det menneskelige led i sikkerhedskæden.
Transparens og rapportering	Sikrer, at ledelse og relevante interessenter regelmæssigt informeres om sikkerhedsstatus, hændelser og forbedringer.
Elasticitet og modstandsdygtighed	Udvikler systemer og processer, der kan modstå og hurtigt genoprette fra sikkerhedshændelser, herunder katastrofer, for at sikre forretningskontinuitet.

Tabel 4.1 - Grundlæggende principper

4.4 Lovgivning og standarder

Som et led i opretholdelsen af Banedanmarks ledelsessystem for informationssikkerhed (ISMS) ønsker Banedanmark at være proaktive i tilgangen til informationssikkerhed og dermed også være proaktive i forhold til at sikre fuld compliance med juridiske, lovmæssige, regulatoriske og kontraktlige forpligtelser, der har relevans for informationssikkerheden i Banedanmark.

Endvidere er det en forudsætning for Banedanmarks virke som infrastrukturforvalter, at Banedanmark tildeles en sikkerhedsgodkendelse fra Trafikstyrelsen. Denne sikkerhedsgodkendelse stiller krav om, at Banedanmark kender den lovgivningsmæssige ramme, som vi skal overholde, ligesom der stilles krav om at vi løbende identificerer lovkrav og andre krav, som skal overholdes[9].

I Banedanmark har Kvalitet & Sikkerhed en proces[10], der sikrer, at vi får identificeret ny eller ændret lovgivning og regler, dels ved hjælp af regelmæssig screening, samt abonnementer på relevante nyhedsbreve. På baggrund af denne vedligeholder Kvalitet & Sikkerhed en liste over alle de lovkrav, der er relevante for Banedanmark, herunder med relevans for informationssikkerhed.

Alle relevante lovkrav til informationssikkerheden i Banedanmark, herunder efterlevede standarder, fremgår af:

- *SL10 Juridiske, lovmæssige, regulatoriske og kontraktlige forpligtelser.*

4.5 ISO/IEC 27001:2023

ISO/IEC 27001 er en international ledelsesstandard for informationssikkerhed. Standarden er et styringsværktøj, der hjælper organisationer til at beskytte værdifulde informationer - herunder også persondata - på en sikker og troværdig måde. ISO 27001 opstiller blandt andet krav til risikostyring, dokumentation af processer, samt fordeling af roller og ansvar for informationssikkerhed.

Formålet med ISO/IEC 27001 er at opnå effektiv informationssikkerhedsledelse, der passer til en virksomheds særlige behov, samt sikre at denne effektivitet fastholdes gennem en proces for løbende forbedring. Det betyder, at informationssikkerheden hele tiden opdateres, således at virksomheden er i stand til at håndtere udfordringerne i en verden under konstant forandring.

ISO/IEC 27001 er valgt som statslig sikkerhedsstandard og har været obligatorisk at følge for statslige institutioner siden januar 2014. Standarden skulle være implementeret af myndighederne primo 2016.

---

[9] Jf. BEK nr 712 af 20/5/2020 - Bekendtgørelse om sikkerhedsgodkendelse, EU-sikkerhedscertifikat og sikkerhedscertifikat på jernbaneområdet, §3, stk. 2 og Bilag 1, afsnit 5.9

[10] Jf. Tracé-proces ST-6.1.2

Som følge af den danske implementering af NIS-direktivet, så har det siden august 2018 været et krav, at Banedanmark ikke bare implementerer og følger standarden, men at Banedanmarks ledelsessystem også opretholder en certificering iht. ISO/IEC 27001.

I december 2021 blev Banedanmark for første gang certificeret iht. den version af standarden, der betegnes ISO/IEC 27001:2013, med opretholdelse af certificeringen forudsætter, at Banedanmark recertificeres hvert 3 år - og dette iht. den seneste udgave af standarden.

Seneste version af standarden er ISO/IEC 27001:2023.

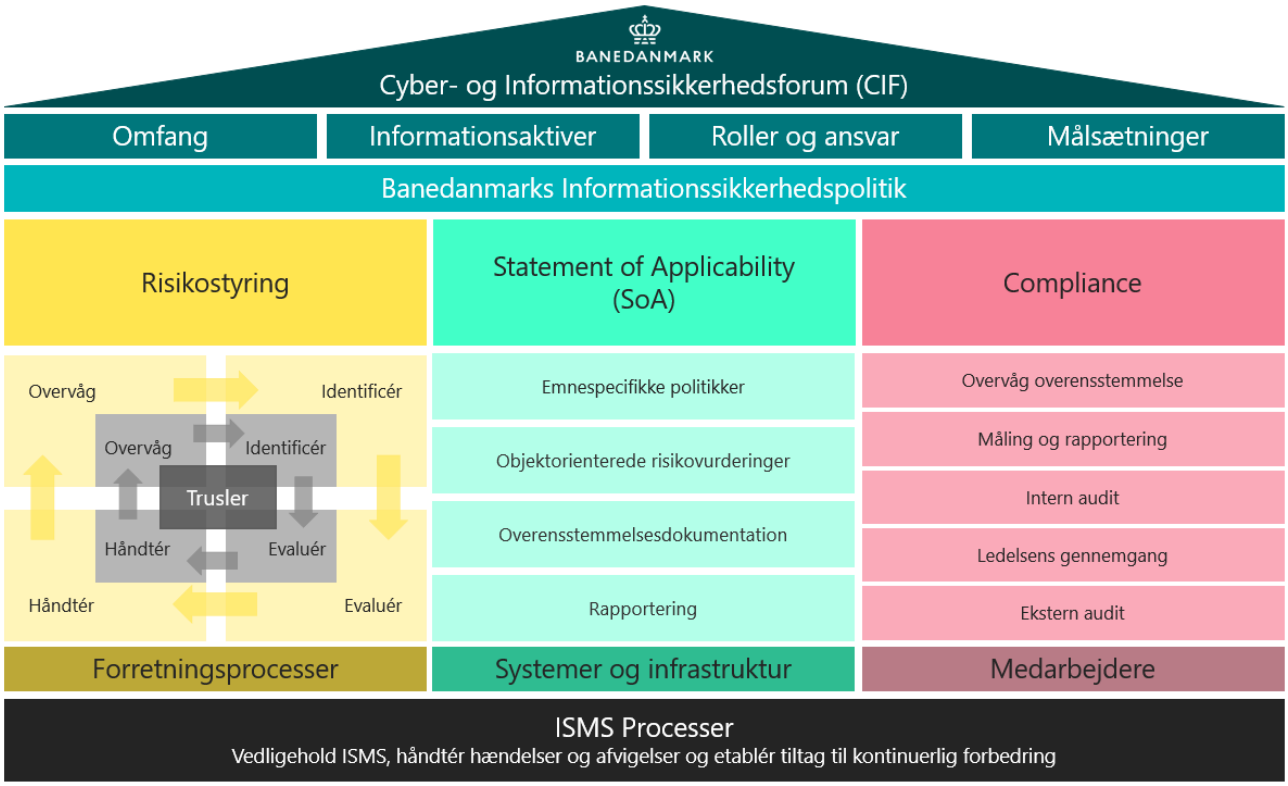
5 ISMS

For at sikre at Banedanmark kan udføre sit hverv, opfylde sine forretningsmæssige mål og overholde sine forpligtelser, er det vigtigt at beskytte informationsaktiverne ved at definere, opnå, vedligeholde og forbedre informationssikkerheden effektivt. Arbejdet med at koordinere og styre disse aktiviteter kaldes informationssikkerhedsledelse.

Når informationssikkerhedsledelse sættes i system sammen med alle de politikker, processer, retningslinjer og ressourcer, som alt sammen baseres på styring af risici, så betegnes det som et ledelsessystem for informationssikkerhed - et Information Security Management System (ISMS).

5.1 Banedanmarks ledelsessystem

Banedanmark har etableret et ledelsessystem for informationssikkerhed (ISMS) i overensstemmelse med de krav, der er specificeret i ISO 27001, som ses illustreret i nedenstående model.

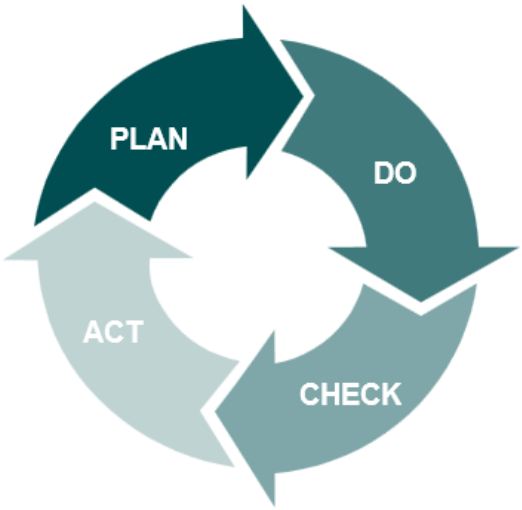


Figur 2. Model for Banedanmarks ISMS

Det øverste niveau i ovenstående model er et ISMS-ledelseslag (■ ■ ■ *i figur 2*), hvori Banedanmarks ISMS defineres og etableres. Det er en række initierende og forberedende aktiviteter, der definerer grundlaget for det fremtidige ISMS, såsom fastlæggelse af kontekst, udarbejdelse af overordnet informationssikkerhedspolitik, fastlæggelse af målsætninger for informationssikkerhed, samt fastlæggelse af roller og ansvar.

Alle øvrige elementer indgår i den proces, der defineres af Banedanmarks ISMS.

I henhold til ISO 27001 skal Banedanmark bl.a. definere og styre ansvaret for informationssikkerheden efter en overordnet proces, der er opbygget efter, og tidligere også var specificeret som, PDCA-modellen (Plan-Do-Check-ACT).



PLAN *(ISO 27001:2023, afsnit 4, 5 og 6)*

- Ansvar for at definere/revurdere behovet for informationssikkerhed ud fra kontekst, interessenter og risici, samt at fastlægge politikker og målsætninger for informationssikkerhed

DO *(ISO 27001:2023, afsnit 7 og 8)*

- Ansvar for at implementere, facilitere, opdatere, kommunikere og dokumentere informationssikkerheden, herunder implementere og styre nødvendige processer og risici

CHECK *(ISO 27001:2023, afsnit 9)*

- Ansvar for at overvåge, måle, analysere, evaluere og auditere informationssikkerheden, samt gennemgå egnethed, tilstrækkelighed og effektivitet af ledelsessystemet

ACT *(ISO 27001:2023, afsnit 10)*

- Ansvar for at håndtere afvigelser og gennemføre og følge op på korrigerende handlinger, samt identificere og planlægge initiativer til løbende forbedring af ledelsessystemet

Figur 3. PDCA-modellen

Anvendelse af PDCA-modellen i Banedanmarks ISMS gennemgås i de nedenstående afsnit.

5.1.1 PLAN - Planlægning af informationssikkerhed

Et af de primære formål med Banedanmarks ISMS er at beskytte Banedanmarks forretningsprocesser og informationsaktiver.

Planlægning handler derfor primært om risikostyring (*i figur 2*) på de kritiske forretningsprocesser og informationsaktiver. Først når de trusler og risici, der kan påvirke forretningsprocesser og informationsaktiver negativt, er identificeret og vurderet, kan der udarbejdes planer for informationssikkerheden, fx i form af emnespecifikke politikker og retningslinjer.

For yderligere information om de metoder, som Banedanmark anvender til hhv. trusselstyring og risikostyring henvises til nedenstående dokumenter:

- *SL06 Trusselsstyring*
- *SL07 Risikostyring*
- *PP06 Proces for trusselsstyring*
- *PP07 Proces for risikostyring*

I tillæg til ovenstående vil det også være en del af planlægningsdelen, at de overordnede rammer for ISMS, som blev etableret som en del af det forberedende arbejde også bliver gennemgået og evt. korrigeret.

5.1.2 DO - Drift af ISMS

I denne aktivitet (■ ■ ■ *i figur 2*) skal det, der er planlagt i afsnit 5.1.1 ovenfor, implementeres og styres i hele Banedanmarks organisation.

Driften af ISMS'et kan derfor opdeles i to hovedindsatser:

Uddannelse, kommunikation, facilitering og vedligeholdelse

- Dette omfatter aktiviteter, der primært håndteres af CIS og handler i princippet om at etablere de bedste betingelser for, at den øvrige organisation kan implementere og vedligeholde det nødvendige niveau for informationssikkerhed. Dette omfatter tydelig kommunikation til den øvrige organisation, uddannelse af ISMS rolle-indehavere, facilitering af implementering, samt vedligeholdelse af ISMS'ets fundament.

Implementere, dokumentere og rapportere

- Her skal informationssikkerheden implementeres og dokumenteres i den øvrige organisation, herunder i forretningsprocesser, på kritiske informationsaktiver og i de tværgående supportfunktioner, der understøtter de kritiske forretningsprocesser, såsom HR, Indkøb, Jura, IT osv. Når implementering og dokumentation er på plads, skal organisationen overvåge, tilpasse og rapportere på informationssikkerheden indenfor deres respektive domæner.

For yderligere information om de ovenstående aktiviteter henvises til nedenstående dokumenter:

- *SL08 Organisering af informationssikkerhed*
- *SL09 Dokumentation af Banedanmarks ISMS*
- *PP01 Årshjul for Banedanmarks ISMS*
- *PP05 Implementeringsproces for systemer og infrastruktur*
- *PP08 Kommunikationsstrategi*

Endvidere er alle de emnespecifikke politikker relevante i forbindelse med implementeringsindsatsen i både systemer og tværgående supportfunktioner.

5.1.3 CHECK - Check af drift

Denne aktivitet (■ ■ ■ *i figur 2*) fokuserer på at evaluere og måle effektiviteten af de handlinger og sikkerhedsforanstaltninger, der bliver implementeret i Drifts-aktiviteten, og sammenligne de faktiske resultater med de oprindeligt forventede mål og målsætninger. Denne kontrol, som fx omfatter overvågning, måling, rapportering, intern og ekstern audit, er afgørende for at identificere afvigelser og områder, der kræver forbedring, og sikrer, at Banedanmarks ISMS kontinuerligt kan forbedres over tid.

For yderligere information om de ovenstående aktiviteter henvises til nedenstående dokumenter:

- *PP01 Årshjul for Banedanmarks ISMS*
- *PP02 Proces for overvågning og forbedring*
- *PP10 Proces for intern audit*

Resultaterne fra denne aktivitet er ikke alene nødvendige for at få afdækket hullerne i Banedanmarks informationssikkerhed og for at CIF kan vurdere effektiviteten af Banedanmarks ISMS, men de anvendes i høj grad i den efterfølgende aktivitet.

5.1.4 ACT - Ageren på check

Denne aktivitet (■ *i figur 2*) sikrer at Banedanmarks ISMS hele tiden bliver bedre og kontinuerligt øger niveauet for Banedanmarks informationssikkerhed. Det er her, hvor Banedanmarks informationssikkerhedsorganisation, baseret på resultaterne fra CHECK-aktiviteten ovenfor, træffer beslutning om at foretage nødvendige forbedringer af ISMS'et. Dette er afgørende for at sikre, at ISMS'et er dynamisk, kan tilpasse sig både interne og eksterne ændringer, og forbedre informationssikkerhedsprocesserne kontinuerligt over tid.

For yderligere information om de ovenstående aktiviteter henvises til nedenstående dokumenter:

- *PP01 Årshjul for Banedanmarks ISMS*
- *PP02 Proces for overvågning og forbedring*
- *PP03 Proces for håndtering af informationssikkerhedshændelser*
- *PP04 Proces for dispensationer*
- *PP05 Implementeringsproces for systemer og infrastruktur*
- *PP11 Proces for håndtering af afvigelser*

Da denne aktivitet også er den sidste i PDCA-cyklussen, så afsluttes aktiviteten med en grundig evaluering af ISMS'et, dets dokumenter og dets effektivitet. Dette danner grundlaget for den næste PDCA-cyklus, hvor Banedanmarks ISMS igen starter ved PLAN-aktiviteten i afsnit 5.1.1 ovenfor.

5.2 Organisering af ledelsessystem

At stille kompetente ressourcer til rådighed for Banedanmarks ISMS er afgørende for at sikre en effektiv og struktureret tilgang til informationssikkerheden. Fastlæggelse af de roller, der indgår i sikkerhedsorganisation, samt præcisering og tildeling af ansvar og opgaver er en betingelse for at ledelsessystemet kan definere, opnå, vedligeholde og forbedre informationssikkerheden effektivt.

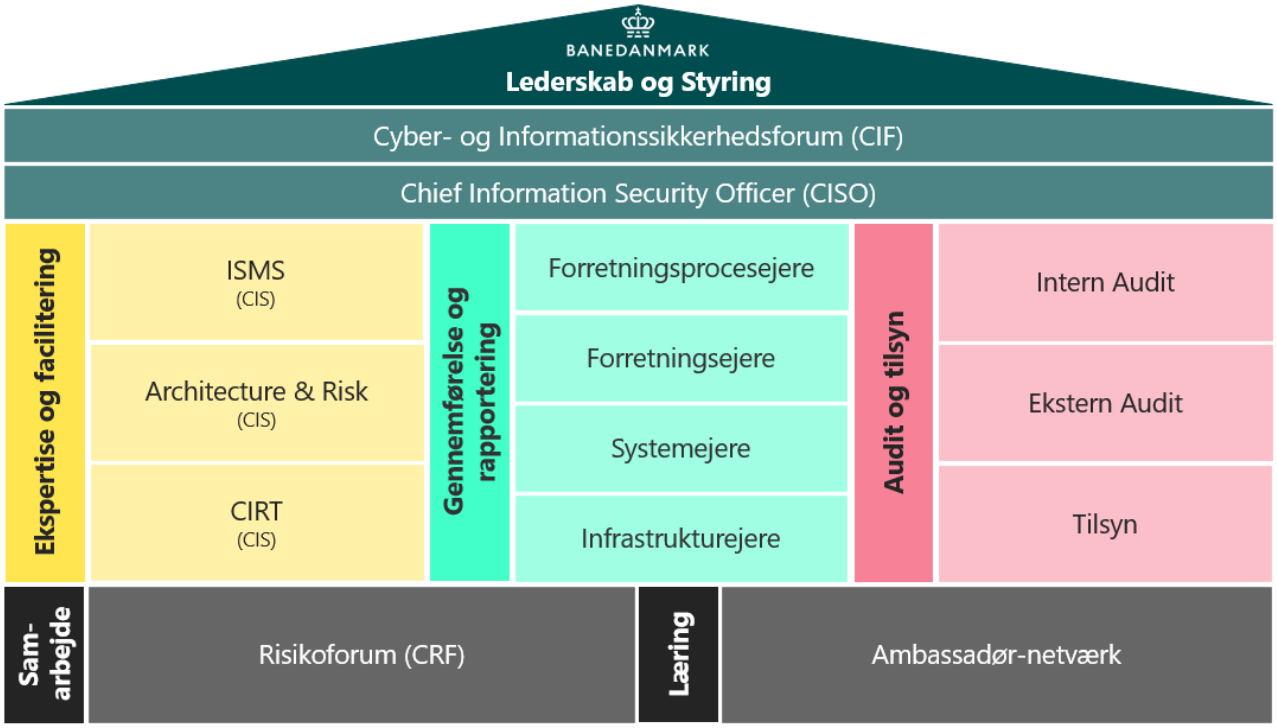
5.2.1 Roller i Banedanmarks ISMS

Banedanmarks direktion bærer ansvaret for informationssikkerheden i Banedanmark, herunder tilgængelighed, integritet og fortrolighed af Banedanmarks informationsaktiver og -systemer.

Til at varetage den overordnede styring og koordinering af ledelsessystemet har Banedanmarks direktion etableret et ledelsesudvalg, Cyber- og Informationssikkerhedsforum (CIF), og udstyret dette med nødvendig autoritet til at lede og fordele arbejdet med informationssikkerhed i Banedanmark.

Til at varetage den daglige styring og koordinering af ledelsessystemet har CIF ansat en Chief Information Security Officer (CISO), som også varetager den daglige ledelse af Banedanmarks Cyber- og Informationssikkerhedssektion (CIS), som skal facilitere og rådgive om ISMS'et og om informationssikkerhed generelt.

Under CIF og CISO er der defineret en sikkerhedsorganisation for Banedanmarks ISMS, som skal varetage de mange aspekter af informationssikkerhedsarbejdet i Banedanmark. Denne sikkerhedsorganisation er, som det fremgår af nedenstående figur, opdelt i en række roller, der samlet set sikrer, at Banedanmarks ISMS opfylder de mål, som CIF sætter for ledelsessystemet.



Figur 4. Roller i Banedanmarks ISMS

En nærmere beskrivelse af ovenstående organisation, herunder af roller, ansvar og opgaver, samt nødvendige kompetencer, fremgår af dokumentet:

- *SL08 Organisering af informationssikkerhed*

5.2.2 Informationssikkerhedsansvar udenfor ISMS-roller

5.2.2.1 Ledelsesansvar

I Banedanmark er det et ledelsesansvar at sikre, at alle medarbejdere er bevidste om og lever op til deres informationssikkerhedsansvar. Som leder i Banedanmark er det væsentligt, at man er bevidst om, at informationssikkerhedsledelse indgår i alle de fire ledelsesdiscipliner[11]. Særligt indenfor Driftsledelse og Faglig ledelse, er det væsentligt, at ledere med udgangspunkt i Banedanmarks politikker, retningslinjer og instrukser bærer ansvar for, at disse efterleves indenfor deres eget ansvarsområde.

5.2.2.2 Medarbejderansvar

Tilsvarende har alle ansatte i Banedanmark et ansvar for at bidrage til en god informationssikkerhed og kan med en fornuftig adfærd hjælpe til med at

[11] Jf. Banedanmarks Ledelsesgrundlag

beskytte Banedanmark mod sårbarheder, utilsigtede sikkerhedshændelser og brud på informationssikkerheden.

Som ansat i Banedanmark har man selv pligt til at sætte sig ind i og følge Banedanmarks Informationssikkerhedspolitik. Informationssikkerhedspolitikken er udmøntet i en række emnespecifikke politikker, som samlet set er med til at skabe et passende informationssikkerhedsniveau i Banedanmark.

Alle medarbejdere skal ved ansættelse gennemføre et obligatorisk online-kursus i informationssikkerhed.

5.2.2.3 Eksterne samarbejdspartnere og konsulenter

I lighed med Banedanmarks ansatte, forventes det også af Banedanmarks eksterne samarbejdspartnere og konsulenter, at de medvirker til at opretholde og fremme informationssikkerheden i Banedanmark.

Alt eksternt personale har ansvar for at sætte sig ind i, forstå og overholde Banedanmarks informationssikkerhedspolitikker og -processer, herunder at gennemføre alle relevante informationssikkerhedsuddannelsesprogrammer og -sessioner, som Banedanmark stiller til rådighed, for at sikre, at de er opdaterede med de seneste sikkerhedspraksisser og -politikker.

I tillæg hertil, har alle eksterne medarbejdere også ansvar for omgående at rapportere eventuelle observerede informationssikkerhedshændelser,[12] mistanker om sikkerhedsbrud eller sårbarheder til Banedanmarks informationssikkerhedsafdeling eller til deres ansvarlige i Banedanmark.

5.3 Dokumenter i ISMS

Banedanmarks ISMS er etableret og certificeret i overensstemmelse med ISO 27001 og skal derfor som minimum have udarbejdet den dokumentation, der kræves af standarden og have den tilgængelig.

I Banedanmark er denne dokumentation planlagt, udarbejdet og præsenteret i en struktur, som er tilpasset Banedanmarks organisation og kontekst, og i sammenhæng med evt. øvrig dokumentation, der vurderes relevant for informationssikkerheden.

Den samlede dokumentation omfatter bl.a.:

- Styrings- og ledelsesdokumenter
- Emnespecifikke politikker
- Processer og procedurer
- Skabeloner og værktøjer
- Overensstemmelsesdokumentation

Alle dokumenter, der indgår i Banedanmarks ISMS, fremgår af:

- *SL09 Dokumentation af Banedanmarks ISMS*

Dokumentet giver en kort beskrivelse af hvert dokument, der indgår i ISMS, med reference til ISO 27001:2023, samt et link til dokumentet.

[12] Defineres som en handling el. hændelse, der negativt påvirker tilgængelighed, integritet eller fortrolighed af Banedanmarks data, systemer, digitale netværk eller digitale tjenester.

6 Leverandørers informationssikkerhed

Gennem EU's vedtagelse af NIS-direktivet[13], og den efterfølgende danske lovmæssige implementering heraf, er Banedanmark lovmæssigt forpligtet[14] til at vedligeholde et højt niveau af informationssikkerhed, der styres af et ledelsessystem for informationssikkerhed (ISMS) i overensstemmelse med ISO 27001:2023.

Jf. direktivet leverer Banedanmark "*en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige og/eller økonomiske aktiviteter*", og hvor en betydelig afbrydelse kan påvirke ikke bare Danmark, men unionen som helhed, bl.a. grundet jernbaneinfrastrukturens tværnationale karakter.

Det forventes derfor også, at alle Banedanmarks leverandører deler denne forpligtelse, dels ved at anerkende vigtigheden af og aktivt arbejde hen imod overholdelsen af Banedanmarks informationssikkerhedspolitik, og dels ved at implementere passende sikkerhedsforanstaltninger, der svarer til dem, Banedanmark anvender internt, for at beskytte de data og systemer, de har adgang til eller forvalter på Banedanmarks vegne.

At være leverandør til Banedanmark betyder derfor at:

- *Leverandører skal regelmæssigt demonstrere deres overensstemmelse med Banedanmarks informationssikkerhedspolitik gennem selv-evalueringer og, hvor det er relevant, eksterne audits.*
- *Leverandører accepterer ved kontraktindgåelse uden unødigt ophold at underrette Banedanmark om eventuelle sikkerhedsbrud eller -svagheder, der kan påvirke kontraktens serviceydelser eller Banedanmarks informationsaktiver.*
- *Banedanmark forbeholder sig ret til at anmode om og modtage rapporter om informationssikkerhedsforanstaltninger og -praksisser fra alle leverandører, samt at foretage revisioner eller inspektioner for at bekræfte overholdelsen på ressourcer, der anvendes i Banedanmark regi.*
- *Leverandører skal arbejde åbent og proaktivt med Banedanmarks informationssikkerhedssektion (CIS) for at løse eventuelle identificerede informationssikkerhedsrelaterede problemer.*
- *Leverandører, der anvender underleverandører til at levere dele af tjenesten, skal sikre, at disse underleverandører også overholder Banedanmarks informationssikkerhedspolitik.*
- *Denne politik er dynamisk og vil blive revideret løbende. Leverandører skal forpligte sig til at følge disse ændringer og justere deres sikkerhedsforanstaltninger i takt med opdateringer af politikken.*

[13] EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen

[14] LOV nr 441 af 8/5/2018 - Lov om sikkerhed i net- og informationssystemer i transportsektoren, samt BEK nr 1042 af 6/8/2018 - Bekendtgørelse om sikkerhed i net- og informationssystemer i transportsektoren

Banedanmarks leverandører bør desuden være opmærksomme på, at alle leverandører, der:

1. *enten beskæftiger over 50 personer, og som har en årlig omsætning eller en årlig samlet balance på over 10 mio. EUR[15],*
2. *eller leverer en tjeneste, der "vil kunne medføre en væsentlig systemisk risiko, navnlig for sektorer, hvor en sådan forstyrrelse kan have en grænseoverskridende virkning" som fx jernbaneinfrastrukturen[16],*
3. *eller "er kritisk på grund af sin specifikke betydning på nationalt eller regionalt plan for den pågældende sektor", her forstået jernbanesektoren[17],*

vil være omfattet af NIS 2 direktivet og de krav til informationssikkerhed, der følger heraf, når direktivet implementeres ved dansk lov.

[15] Virksomheder, der jf. EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet), artikel 2, stk. 1, overskrider tærsklerne for små virksomheder (jf. KOMMISSIONENS HENSTILLING 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder, Bilagets artikel 2, stk. 2).

[16] jf. EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet), artikel 2, stk. 2, litra d).

[17] jf. EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet), artikel 2, stk. 2, litra e).

7 Informationssikkerhedshændelser

Banedanmarks tilgang til håndtering af informationssikkerhedshændelser er baseret på proaktiv identifikation, hurtig rapportering, grundig analyse og effektiv håndtering af alle informationssikkerhedshændelser for at beskytte informationsaktiver og opretholde en kontinuerlig drift.

7.1 Rapportering af informationssikkerhedshændelser

Alle i Banedanmark, herunder samtlige medarbejdere uanset niveau, konsulenter, og eksterne medarbejdere, der er kontraktuelt tilknyttet til Banedanmark, har pligt til at indberette informationssikkerhedsbrud, sårbarheder eller sikkerhedshændelser.

En informationssikkerhedshændelse er en samlet betegnelse for alle de forskellige typer af tekniske og menneskeskabte uheld/brud, der kan udgøre en risiko for de informationer og data, der behandles af Banedanmark. Dette gælder både for digitale og fysiske informationer og data. Det kan fx være informationer og data, der fejlagtigt slettes, ændres eller videregives til de forkerte. Det kan være utilsigtet (en fejl) eller tilsigtet (fx hacking).

Også forhold, der ville kunne lede til et informationssikkerhedsbrud (fx en dør ind til et datacenter med kode/adgangskontrol, der ikke lukker, eller en leverandør til Banedanmark, der ved en fejl sender et brugernavn og password via usikker kommunikation som f.eks. e-mail). Sådanne forhold kaldes bl.a. for sårbarheder.

Bliver du opmærksom på noget, der kan have betydning for informationssikkerheden, fx informationssikkerhedsbrud, sårbarheder eller andet, skal du øjeblikkeligt kontakte Servicedesk på e-mail 14700@bane.dk eller tlf.: 8234 4700.

I tillæg til ovenstående, er Banedanmark underlagt en forpligtelse til hurtigst muligt uden ophold - og senest inden udgangen af førstkommende hverdag - at underrette om hændelser, der vurderes at kunne have konsekvenser for kontinuiteten af togdriften[18].

7.2 Håndtering af informationssikkerhedshændelser

Generelt ligger håndtering af informationssikkerhedshændelser i direkte forlængelse af systemspecifikke incident management-processer. I situationer, hvor der er tale om informationssikkerhedshændelser uden for de

[18] Jf. BEK nr 1042 Bekendtgørelse om sikkerhed i net- og informationssystemer i transportsektoren, §8, stk. 1.

informationsaktiver, der er specificeret i SL05 Fortegnelse over kritiske informationsaktiver, håndteres informationssikkerhedshændelser iht. følgende dokument:

- *PP03 Proces for håndtering af informationssikkerhedshændelser.*

Hvor der anvendes systemspecifikke processer for incident management, skal det kunne dokumenteres, at processerne særskilt identificerer informationssikkerhedshændelser og håndterer dem efter følgende model:

**) I situationer, hvor der er tale om en cybersikkerhedshændelse, er det dog meget væsentligt, at man som det allerførste kontakter Banedanmarks Cyber Incident Response Team (CIRT), inden man forsøger at stoppe hændelsen.*

Figur 5. Model for hændelseshåndtering.

Ved udarbejdelse af hændelsesrapport er et krav, at Banedanmarks rapporteringsskabelon for informationssikkerhedshændelser anvendes.

- *SV09 Skabelon for rapportering af informationssikkerhedshændelser*

Yderligere rådgivning/vejledning kan fås ved at kontakte sektionen for Cyber- og informationssikkerhed (CIS) på informationssikkerhed@bane.dk.

7.3 Forretningskontinuitet og beredskab

Som infrastrukturforvalter af en samfundskritisk infrastruktur er Banedanmark ved lov påbudt at "*træffe passende foranstaltninger for at forebygge og minimere konsekvensen af hændelser, der berører sikkerheden i net- og informationssystemer, som anvendes til levering af sådanne væsentlige tjenester, med henblik på at sikre kontinuiteten i disse tjenester*"[19].

Alle systemer/informationsaktiver, som er underlagt Banedanmarks ISMS[20] er derfor pålagt at udarbejde planer for at sikre genopretning efter alvorlige hændelser under behørig hensyntagen til forretningskontinuitetsforanstaltninger og dermed genoptage leveringen af de services, som systemet/informationsaktivet leverer.

For hvert kritisk system vil der være udarbejdet følgende:

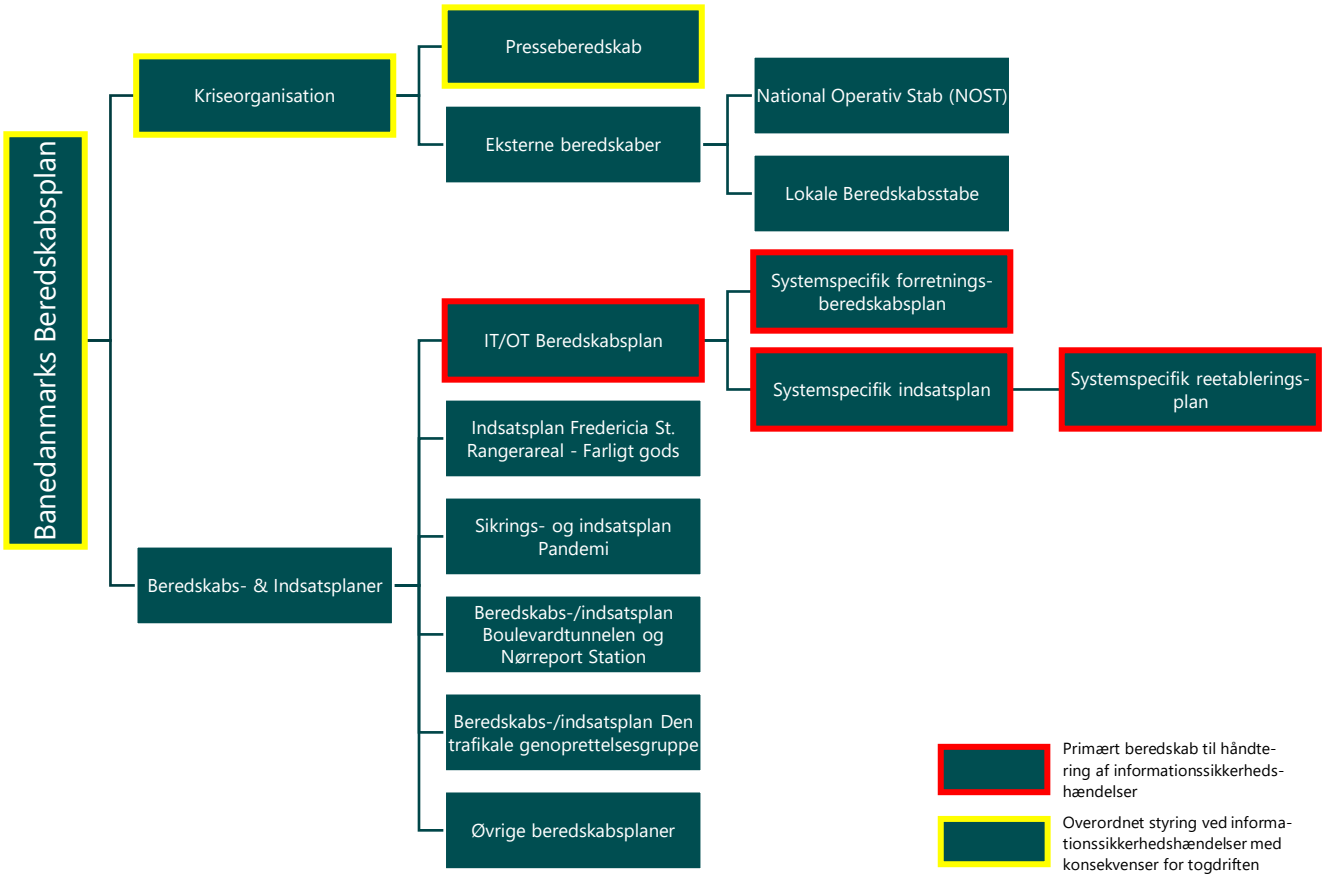
[19] Jf. EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen, artikel 14, stk. 2

[20] Jf. SL05 Fortegnelse over kritiske informationsaktiver

Figur 6. Dokumenter ifm. beredskab ved informationssikkerhedshændelser.

I tilfælde af en alvorlig hændelse på et enkelt kritisk system skal både Forretningsejer og Systemejer orienteres, hvorefter de træffer beslutning om, hvorvidt deres respektive planer skal aktiveres.

Såfremt den alvorlige hændelse ikke blot påvirker et enkelt kritisk system, men derimod en mængde kritiske systemer, så indgår de systemspecifikke planer som en del af et større beredskabskompleks, der koordineres af Kvalitet & Sikkerhed, som derfor skal orienteres og herefter træffer beslutning om, hvorvidt Banedanmarks generelle beredskabsplan skal aktiveres.



Figur 7. Banedanmarks Beredskabskompleks

8 Løbende forbedring

Udover, at ISO 27001 stiller krav om kontinuerlig forbedring af ISMS'et[21], så er en løbende forbedring af Banedanmarks ISMS en helt grundlæggende forudsætning for at sikre, at Banedanmarks informationssikkerhedsforanstaltninger forbliver effektive og relevante over tid.

Ved at have et kontinuerligt fokus på at forbedre Banedanmarks ISMS, så sikres det, at ISMS'et, og Banedanmark generelt, ikke kun opfylder de nuværende sikkerhedsbehov, men også proaktivt tilpasser sig fremtidige trusler, teknologiske fremskridt og ændringer i den organisatoriske kontekst.

Kontinuerlig forbedring foregår som beskrevet i afsnit 5.1.4 ovenfor i den sidste del af PDCA-cyklussen.

Yderligere information om arbejdet med løbende forbedring af Banedanmarks ISMS fremgår af dokumentet:

- *PP02 Proces for overvågning og forbedring*

[21] Se DS/EN ISO/IEC 27001:2023, klausul 10.1

9 Overensstemmelse og revision

En vigtig forudsætning for, at Banedanmarks ISMS kan fungere effektivt og blive ved med at gøre dette over tid, er, at der gennemføres løbende, uafhængig kontrol og tilsyn for at sikre, at politikker, procedurer og sikkerhedsforanstaltninger er i overensstemmelse med kravene i Banedanmarks ISMS og med ISO 27001 standarden - og er effektive i forhold til at opnå de planlagte resultater.

9.1 Revision og certificering

Iht. ISO 27001:2023, klausul 9.2, skal Banedanmark gennemføre uafhængige, interne audits for at gennemse og evaluere, hvorvidt Banedanmarks ISMS er implementeret og fungerer.

Banedanmarks interne auditfunktion er organisatorisk placeret i Kvalitet & Sikkerhed.

Herudover foreskriver den danske lovgivning også, at Banedanmark skal opnå og opretholde en akkrediteret certificering i overensstemmelse med en internationalt anerkendt standard[22], som siden januar 2014, har været ISO 27001 for alle statslige myndigheder[23].

Certificering, løbende overvågning og recertificering af Banedanmarks ISMS's overensstemmelse med ISO 27001 foretages gennem regelmæssige audits fra en ekstern certificeringsmyndighed.

For yderligere information om intern og ekstern audit se:

- *SL08 Organisering af informationssikkerhed*
- *PP10 Proces for intern audit*

9.2 Tilsyn

Som en offentlig styrelse under Transportministeriet er Banedanmark underlagt tilsyn fra øvrige offentlige myndigheder. Disse myndigheder har beføjelse til at overvåge Banedanmarks overholdelse af gældende love og reguleringer inden for informationssikkerhed.

Banedanmark er underlagt forskellige tilsyn, heriblandt det fællesstatslige tilsynskoncept, tilsyn fra Digitaliseringsstyrelsen og Rigsrevisionen.

For yderligere information om intern og ekstern audit se:

- *SL08 Organisering af informationssikkerhed*

[22] Jf. BEK nr 1042 af 06/08/2018 Bekendtgørelse om sikkerhed i net- og informationssystemer i transportsektoren, §5.

[23] Jf. "Enkel administration i staten", januar 2010, side 49.

Appendix 1 Emnespecifikke politikker

Generelt skal fastlæggelse og implementering af informationssikkerhedsforanstaltninger i Banedanmark ske på baggrund af en risikovurdering af det informationsaktiv, der skal beskyttes. På baggrund af den udarbejdede risikovurdering fastlægges en systemspecifik SoA[24].

For at sikre en beskyttelse af informationsaktiver, der er tilpasset den vurderede størrelse på de risici, som er gældende for informationsaktiverne, har Banedanmark defineret en række emnespecifikke informationssikkerhedspolitikker, der hver især fastsætter en række overordnede krav, der kan tilpasses i overensstemmelse med det behov for beskyttelse, som en korrekt håndtering de identificerede risici fordrer.

De emnespecifikke politikker håndterer samlet set de informationssikkerhedsforanstaltninger, der fremgår af ISO 27001:2023, Anneks A.

Nedenstående er en oversigt over alle emnespecifikke politikker, og de kan enten findes på Banedanmarks intranet, Baneinfo, eller udleveres ved henvendelse til Banedanmarks Cyber- og Informationssikkerhedssektion (CIS).

Titel på politik	Beskrivelse	ISO 27001:2023 Anneks A
Emnespecifikke politikker		
EP01 Politik for ISMS Governance	Dette dokument beskriver dels, hvordan Banedanmarks ISMS er opbygget og dels hvordan Banedanmarks ISMS skal driftes og vedligeholdes.	*A.5.1-A.5.6*
EP02 Politik for styring af aktiver	Dette dokument beskriver, hvordan informationsaktiver registreres og forvaltes i Banedanmark med et primært fokus på informationsaktiver, hvortil brugerne har adgang.	*A.5.9, A.5.10, A.5.11, A.6.7 og A.8.1*
EP03 Politik for informationssikkerhed i projekter	Dette dokument fastlægger retningslinjer for, hvordan arbejdet med informationssikkerhed integreres i projekter.	*A.5.8*
EP04 Politik for sikker udvikling	Dette dokument beskriver, hvordan Banedanmark sikrer højeste kvalitet og informationssikkerhed i al udvikling af software og systemer i regi af Banedanmark.	*A.8.25 - A.8.31*
EP05 Politik for informationssikkerhed i leverandørstyring	Dette dokument fastlægger de informationssikkerhedsmæssige rammer og krav til Banedanmarks samarbejde med leverandører, både med hensyn til styring og leverancer.	*A.5.19 - A.5.23*
EP06 Politik for sikker informationsforvaltning	Dette dokument angiver de overordnede retningslinjer for beskyttelse af information i Banedanmark, herunder retningslinjer for klassifikation og beskyttelse af information.	*A.5.12, A.5.13, A.5.14, A.8.10, A.8.11, A.8.12, A.8.33 og A.8.34*
EP07 Politik for fysisk sikkerhed	Denne politik beskriver Banedanmarks krav til implementering af foranstaltninger, der beskytter den fysiske sikkerhed for Banedanmarks informationsaktiver, herunder IT-systemer, operationelt udstyr, samt infrastruktur som fx fysiske lokationer.	*A.7.1 - A.7.14*
EP08 Politik for informationssikkerhed på HR-området	Dette dokument beskriver Banedanmarks politikker for at evt. trusler der kan relateres til Banedanmarks medarbejdere, som jo også er et informationsaktiv for Banedanmark, også håndteres præventivt.	*A.6.1, A.6.2, A.6.3, A.6.4, A.6.5 og A.6.6*

[24] Se SL04 Banedanmarks efterlevelseserklæring

Titel på politik	Beskrivelse	ISO 27001:2023 Anneks A
EP09 Politik for adgangsstyring	Dette dokument sætter en overordnet ramme for adgangsstyring i forhold til Banedanmarks forretningsaktiver og faciliteter, herunder bl.a. informationer, applikationer, systemer og netværk.	*A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3, A.8.4 og A.8.5*
EP10 Politik for lovgivning og compliance	Dette dokument fastlægger de rammer for informationssikkerhedsarbejdet, som Banedanmark pålægges gennem lovgivning, regulativer, kontrakter og andre eksterne, styrende dokumenter, som fx koncernstrategier m.m.	*A.5.31, A.5.32, A.5.33, A.5.34, A.5.35 og A.5.3*
EP11 Politik for netværkssikkerhed	Dette dokument fastlægger retningslinjer for styring, dokumentation og kontrol af netværk med henblik på at sikre beskyttelse af informationer i systemer og applikationer, samt i de understøttende informationsbehandlingsfaciliteter.	*A.8.7, A.8.20, A.8.21, A.8.22 og A.8.23*
EP12 Politik for styring af informationssikkerhedshændelser	Denne politik er et supplement til Banedanmarks proces for håndtering af informationssikkerhedshændelser og fastlægger krav vedrørende planlægning i tilfælde af, overvågning for, rapportering af, vurdering af, håndtering af, dokumentation af og læring fra informationssikkerhedshændelser.	*A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.8, A.8.15, A.8.16 og A.8.17*
EP13 Politik for beredskab og kontinuitet	Dette dokument beskriver krav til den overordnede planlægning, implementering, håndtering, vedligeholdelse og eksekvering af beredskab relateret til samfundskritiske forretningsprocesser og informationsaktiver.	*A.5.29, A.5.30, A.8.6, A.8.13 og A.8.14*
EP14 Politik for sikker IT-drift	Dette dokument definerer Banedanmarks forståelse af sikker IT-drift og fastlægger i forlængelse heraf de krav, der stilles til planlægning, drift og vedligeholdelse af IT-systemer.	*A.5.37, A.8.6, A.8.8, A.8.9, A.8.19, A.8.24 og A.8.32*