Informationssikkerhedspolitik 28.02.2017

banedanmark

Banedanmark
IT
Amerika Plads 15
2100 København Ø
www.banedanmark.dk

Forfatter: Carsten Stenstrøm
Mail: cstr@bane.dk
Telefon: 41881976

Informationssikkerhed

Indhold Side

1 Informationssikkerhedspolitik

1.1 Indledning

Denne informationssikkerhedspolitik fastsætter den overordnede ramme for informationssikkerheden i Banedanmark. Informationssikkerhedspolitikken udgør grundlaget for den daglige styring af informationssikkerhed i Banedanmark. Ansvarsplacering, retningslinjer, procedurer, risikovurdering, og it-beredskabsplaner er således emner, der reguleres under denne overordnede politik.

Banedanmarks informationssikkerhed er baseret på den påkrævede ISO 27000 standard, som fastsætter de styringsmæssige principper for informationssikkerhed.

1.2 Definition og omfang

Informationssikkerhed defineres som de sikkerhedsforanstaltninger, der har til formål at beskytte samtlige informationer. Informationssikkerhedspolitikken omfatter alle Banedanmarks informationer, uanset i hvilken form de opbevares og på hvilken måde de formidles.

Alle leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til systemer, data og informationer skal gøres bekendt med politikken og følge den.

1.3 Formål

Banedanmark er afhængig af, at informationer og informationssystemer er tilgængelige, og informationssikkerhedspolitikken har derfor vital betydning for Banedanmarks daglige virke.

Politikken skal understøtte 3 hovedområder:

Tilgængelighed af data:

At opnå den aftalte tilgængelighed (oppetid) med minimeret risiko for nedbrud.

Integritet af data:

At opnå pålidelige og korrekte data og minimere interne og eksterne hændelser.

Fortrolighed af data:

I fornødent omfang at sikre fortrolig behandling, transmission og opbevaring af informationer.

1.6 Sikkerhedsbevidsthed

Banedanmark ønsker at beskytte sine data og informationer, således at anvendelse og adgang, herunder offentliggørelse af informationer, skal ske i overensstemmelse med virksomhedens retningslinjer og under hensyntagen til den til enhver tid gældende lovgivning.

Banedanmark ønsker at tilrettelægge niveauet for datasikkerheden med fornøden fleksibilitet, så den tilgodeser krav om at kunne arbejde på tværs af Banedanmarks forskellige geografiske steder, og at rådgivere/entreprenører kan samarbejde om projekter med relevant personale uden it-barrierer. Dette skal ske samtidig med, at organisationens samlede sikkerhedsniveau for kritiske systemer sikres udadtil og med balanceret sikkerhed indenfor de pågældende samarbejdsområder.

Banedanmark fastlægger sikkerhedsniveauet på baggrund af en risikovurdering, som foretages gennem en afvejning af omkostninger til sikkerhedsforanstaltninger i forhold til de risici, der er forbundet med manglende sikkerhed. Gældende lovkrav og bekendtgørelser skal overholdes.

Overordnet risikovurdering gennemføres, således at ledelsen kan forholde sig til det aktuelle sikkerhedsniveau og ændringer heraf.

Det ønskede sikkerhedsniveau for data og dermed informationer i Banedanmark er:

Tilgængelighed af data: Højt niveau

Banedanmark er afhængig af at da et tilgængelige på en højt niveau med få og begrænsede afbrydelser for at sikre effektiv drift og information For de informationsaktiver, der anvendes til jernbanesikkerhed, herunder Signalprogrammet, er sikkerhedsniveauet for integritet **høj**.

Integritet af data: Højt niveau

Datas korrekthed er fundamentet i styring af Banedanmarks driftsaktiviteter og informationssystemer.

Fortrolighed af data: Middel niveau

Banedanmark overholder lovgiving. Anvendelse af persondata anvendes kun i fornødent omfang til HR relaterede områder og grænseflader med leverandører.

Beskyttelse af IP(rettigheder) er en naturlig del af produktionen.

1.5 Ledelsens støtte og engagement

Banedanmarks ledelse vil udvise støtte og engagement til gennemførelse af tiltag

1.6 Sikkerhedsbevidsthed

til understøttelse af informationssikkerheden.

Ligeledes skal ledelsen medvirke til fastsættelse af risikoaccept, hvor tekniske eller organisatoriske forhold umuliggør implementering af sikringstiltag.

Banedanmarks ledelse vil oplyse medarbejderne om ansvarlighed i relation til Banedanmarks informationer og informationssystemer.

Alle medarbejdere har ansvar for at bidrage til at beskytte Banedanmarks informationer mod uautoriseret adgang og ændring samt tyveri.

Alle medarbejdere skal modtage uddannelse og informeres om informationssikkerhed i relevant omfang. Alle medarbejdere modtager senest på første arbejdsdag virksomhedens sikkerhedsregler og kvitterer for at ville følge dem.

Alle brugere af Banedanmarks informationer, såvel interne som eksterne, skal følge de fastsatte regler.

Sikkerhedsbevidsthed skal tænkes ind, når nye systemer implementeres.

1.7 Ansvar for informationssikkerheden

Banedanmarks adm. direktør har det overordnede ansvar for informationssikkerheden. Dette ansvar er delegeret til økonomidirektøren og it-chefen, som har udpeget en informationssikkerhedschef. Denne har ansvaret for styring og implementering af Banedanmarks informationssikkerhed.

Informationssikkerhedschefen har ret og pligt til proaktivt at informere direktionen, hvis der opstår kritiske situationer.

Ledelsen har ansvaret for, at retningslinjer for informationssikkerheden følges og at medarbejderne instrueres herom.

Styring af informationssikkerheden er beskrevet i ”Styringsmodel for informationssikkerhed".

1.8 Brud på informationssikkerheden

Enhver medarbejder, som bliver bekendt med brud på informationssikkerheden, har pligt til at meddele dette til informationssikkerhedschefen.

1.9 Kontrol og revision

Direktionen, Rigsrevisionen, it-ledelsen og informationssikkerhed kan beslutte, om der skal foretages yderligere kontrol og revision.

1.10 Godkendelse & Historik

Håndtering af ændringer i sikkerhedsdokumentationen foretages på følgende måde:

- Informationssikkerhedspolitikken: Godkendes af ledelsen.
- Informationssikkerhedshåndbogen samt bilag og retningsliner.
- Operationelle procedurer: Kan foretages af de ansvarlige medarbejdere.

Informationssikkerhedspolitikken er senest godkendt af Banedanmarks direktion den 26. juni 2015, og træder i kraft med øjeblikkelig virkning.

Revision	Ændring:	Dato	Forfatter
01.03	Betydning af sikkerhedsniveau uddybes og der fokuseres på data fremfor systemer.	23.03.17	CSTR
01.02	Opdatering af format og indholdstekst. Herunder sammensluttet afsnittene 'Definition' og 'Omfang' til et enkelt afsnit og tilføjet en specificering af omfang med grøn farve. Ændringsprocedure med grøn farve og Historik tilføjet i slutningen af dokumentet. Yderligere er al rød tekst indskrevet de steder hvor det var ønsket.	19.02.16	HJMT
01.01	Opdatering af indholdstekst i overensstemmelse med sikkerhedsstandarden ISO27000. Indsat direktørgruppemødets forslag til tilføjelser i rød tekst.	28.03.14	CSTR