Jyske Bank Politik for It sikkerhed

Indholdsfortegnelse

1. Formål og omfang

Formålet med denne Politik for It sikkerhed (herefter benævnt Sikkerhedspolitikken) er at sikre, at der implementeres og opretholdes et højt It sikkerhedsniveau i Jyske Bank-koncernen, herunder at fastlægge principper og krav til It sikkerhedsstyring og It risikostyring, der sikrer, at It sikkerhedsniveauet og den ønskede risikoprofil på It området kan overholdes.

2. It sikkerhedsniveau

It sikkerhedsniveauet skal fastsættes med udgangspunkt i koncernens ambition om at opnå og vedligeholde et sikkerhedsniveau, som er på niveau med de bedste finansielle institutioner i Norden. Fastsættelse af It sikkerhedsniveauet skal modsvare udviklingen i trusselsniveauet på nationalt plan, baseres på risikovurderinger og efterleve sektorens lovgivning og krav.

Det høje It sikkerhedsniveau skal være med til at gøre koncernen i stand til at oppebære et forsvar imod cybertrusler bestående af effektive teknologiske foranstaltninger, processer og menneskelige ressourcer. Koncernens It systemer og It anvendelse skal sikres en robusthed, som kan sikre stabil drift af koncernens forretningsprocesser samt sikre en cyberrobusthed, som er effektiv over for cyberangreb fra trusselsaktører, der arbejder med høj grad af organisering og sofistikerede angreb.

Sikkerhedspolitikken skal suppleres af en strategi, som beskriver, hvorledes It sikkerhedsniveauet skal opnås. Derudover skal Sikkerhedspolitikken uddybes i understøttende politikker, metodebeskrivelser, rammeværk, forretningsgange og retningslinjer, som beskriver, hvorledes kravene heri operationaliseres.

Kravene, som er defineret i politikker, metodebeskrivelser, rammeværk og forretningsgange, skal til enhver tid efterleves. Afvigelser fra Sikkerhedspolitikken skal risikovurderes. Dispensationer fra Sikkerhedspolitikken skal foreligge for væsentlige afvigelser.

Sikkerhedspolitikken skal godkendes af Jyske Banks koncernbestyrelse minimum én gang årligt eller ved væsentlige ændringer, som fordrer, at den revideres.

3. Organisation og ansvar

Direktionen har det overordnede ansvar for, at Sikkerhedspolitikken efterleves, og denne skal sikre, at organisationen støtter op om Sikkerhedspolitikken ved at udstikke klare retningslinjer, udvise synligt engagement og sikre en præcis placering af ansvar.

Koncernen anvender en "3 Lines of Defense" model til at sikre, at Sikkerhedspolitikken efterleves, og at It operationelle risici håndteres og overvåges. Dette sker igennem flere organisatoriske funktioner i koncernen.

- 1st line udgøres af linjeorganisationen og særligt de organisatoriske funktioner, som arbejder med behandling af informationer, drift og It udvikling.
- 2nd line udgøres primært af sikkerhedsafdelingen (It sikkerhed og –risikostyring), men Compliance funktionen (Compliance) og risikofunktionen (Risikostyring) varetager tillige et 2nd line ansvar i relation til kontrol og overvågning af It operationelle risici, idet der er høj samhørighed imellem

Sikkerhedspolitikken, "Politik for Compliance" og "Politik for operationel risikostyring i Jyske Bank koncernen".

- 3rd line udgøres af Intern Revision, der har ansvaret for at udføre uafhængig revision af den samlede håndtering af risici og de interne kontroller i koncernen – samt rapportere om sit arbejde til bestyrelsen.

4. It risikostyring

Koncernens eksponering over for It operationelle risici skal overvåges og rapporteres til ledelsen. Håndteringen af It operationelle risici skal overholde og understøtte koncernens retningslinjer for håndtering af operationelle risici på tværs af koncernen.

De It operationelle risici identificeres og ejes primært af 1st line. Dermed placeres ansvaret for risikostyring hos de 1st line funktioner, der har mest indsigt i og er tættest på den givne risiko.

Dette betyder, at de har ansvar for:

- at håndtere risici,
- at overvåge udviklingen af risici,
- at sikre sig, at de rette kontroller er til stede og udføres for at reducere risiko og konsekvenser, samt
- at iværksætte initiativer til risikoreduktion.

2nd line skal understøtte 1st line i at overholde deres ansvar ved at bistå med rammeværk, metoder, processer og konsultation, som kan vejlede 1st lines risikohåndtering.
Ydermere skal 2nd line overvåge og kontrollere 1st lines håndtering af risici og sikkerhedsniveauet, herunder være særligt opmærksomme på håndteringen af top risici og verificere kontrollers operationelle udførelse og effektiviteten af kontrollerne.

Metode for håndtering af top risici skal indebære vurdering af den iboende risiko og residual risiko. For risikoscenarier med høj iboende risiko, skal der være en stillingtagen til, i hvor høj grad kontrollernes effektivitet skal verificeres.

5. Outsourcing

Ved outsourcing, herunder videreoutsourcing, til eksterne leverandører skal IT-sikkerhedsniveauet for Jyske Bank opretholdes. Dette er ensbetydende med at sikkerhedsprincipperne i Sikkerhedspolitikken skal efterleves. Enhver outsourcing, såvel af væsentlige som ikke-væsentlige aktivitetsområder, skal registreres centralt for at der løbende kan føres kontrol med leverandørernes IT-sikkerhedsniveau.

6. Sikkerhedsprincipper

Sikkerhedspolitikken understøttes af en række sikkerhedsprincipper, som skal uddybes i supplerende retningslinjer og forretningsgange. De vigtigste principper for overholdelse af denne politik beskrives nedenstående:

1. ***Awareness***
   Løbende information og uddannelse til koncernens medarbejdere omkring It sikkerhed skal sikre en bæredygtig sikkerhedskultur. Der skal foretages vurdering om målrettet It sikkerhedstræning for medarbejdere, som er i berøring med risikofyldte aktiviteter.

2. ***Funktionsadskillelse***
   Funktionsadskillelse skal implementeres og overvåges i tilstrækkeligt omfang til at sikre adskillelse mellem It drift, systemudvikling og forretningsførelse. Funktionsadskillelsen skal sikre, at risikoen for enkelte funktioner eller personer, der udfører væsentlige handlinger, der kan kompromittere sikkerheden, minimeres.

3. ***Risikovurdering***
   Der skal foreligge risikovurderinger til grund for centrale vurderinger og beslutninger, ligesom der skal foreligge risikovurderinger af væsentlige systemer for bankens drift.

   Risikovurderingerne skal give tilstrækkeligt overblik over It operationelle risici samt imødegående kontrol- og sikkerhedsforanstaltninger.

   Datakilder, som giver indsigt i It risici, skal defineres og indgå som del af risikovurderingerne, således It risikostyringsprocessen kontinuerligt optimeres på baggrund af faktiske fejl, problemer og svagheder.

4. ***Beskyttelse af It aktiver***
   It aktiver skal beskyttes mod fysiske og logiske trusler i betryggende omfang.

   Sikkerhedsvurderinger og risikovurderinger skal udføres for at afdække, hvorvidt It aktiver beskyttes i betryggende omfang i forhold til koncernens risikoappetit, samt i henhold til lovgivning om persondatabeskyttelse, hvor risici i forhold til datasubjektet (individet) skal vurderes.

   Driften og effektiviteten af de væsentligste foranstaltninger til at beskytte It aktiver skal opretholdes og i væsentlig omfang verificeres.

   It aktiver skal være sikret af tilstrækkelige logiske og fysiske adgangskontroller.

5. ***Adgange til informationer og systemer***
   Adgangskontroller skal overvåges og logges på en sådan måde, at sporing og efterforskning i forbindelse med sikkerhedsbrud kan foregå i tilfredsstillende omfang.
   Privilegerede brugere skal håndteres særligt restriktivt i forhold til generelle brugere.

   Der skal foreligge klassifikationsmodeller for systemer og data, som giver et tilstrækkeligt overblik over de mest væsentlige It aktiver og adgangene hertil.

6. ***Systemudvikling og vedligeholdelse af systemer***
   Der skal forefindes procedurer, der sikrer, at risici forbundet med udvikling, konfiguration og vedligeholdelse af nye og ændrede systemer identificeres, vurderes og håndteres.

Ændringsstyringsprocedurer skal foreligge i en sådan form, at væsentlige ændringer samt risici forbundet med ændringer og idriftsættelser identificeres, vurderes og håndteres proaktivt som integreret del af udviklingsfasen, og afprøves inden de realiseres i produktion.

Behovet for 2-leddet godkendelse vurderes ved anvendelse af processer, der er underlagt funktionsadskillelsesprincipperne.

Det er et krav, at der udarbejdes og vedligeholdes dokumentation for alle væsentlige systemer og konfigurationer, samt at ændringer hertil risikovurderes og dokumenteres på en måde, der sikrer sporbarhed.

7. *Driftsafvikling*

Der skal til enhver tid være anskaffet tilstrækkelige It ressourcer til at opretholde en sikker drift, herunder personel, maskinel og faciliteter.

Procedurer for hændelsesstyring og problemstyring skal sikre, at It risici identificeres, vurderes og håndteres, og indgår som datakilder i risikostyringsprocessen.

Driften skal afvikles i overensstemmelse med de i denne It sikkerhedspolitik angive krav, samt underbyggende metodebeskrivelser, politikker, retningslinjer og forretningsgange.

8. *Backup og sikkerhedskopiering*

Der skal foretages sikkerhedskopiering og backup af systemer og data.

Hyppigheden for sikkerhedskopiering og backup af systemer og data skal baseres på baggrund af risikovurderinger, der inddrager deres klassifikation.

Sikkerhedskopier og backups skal opbevares sikkert og være utilgængelige for uautoriserede personer og brugere.

9. *Beredskab*

Beredskabsmålsætningen skal som minimum fremgå i It beredskabsplanen.

Beredskabsmålsætningen skal sætte mål for genetablering af normal drift i tilfælde af fejl, nedbrud, tab af data eller systemer, samt hel eller delvis ødelæggelse af bygninger, maskinel og kommunikationsveje.

It beredskabsplanen skal beskrive, hvorledes beredskabsorganisationen er sammensat, samt i hvilke tilfælde den etableres.

It beredskabsplanen skal understøttes af nødplaner, der sikrer, at driften af forretningskritiske processer i et acceptabelt omfang kan opretholdes i tilfælde af systemnedbrud, fejl og forstyrrelser i It anvendelsen.

Forretningskritiske systemer og data skal i overvejende grad være understøttet af flercenterdrift, således at tilgængeligheden sikres i tilfælde af nedbrud ved et datacenter.

Det skal ud fra en risikovurdering fastslås, at den logiske og geografiske afstand mellem driftscentrene er tilstrækkelig til, at en hændelse, der sætter ét driftscenter ud af drift, ikke kan ramme øvrige driftscentre samtidigt.

Der skal afholdes regelmæssige beredskabstests og –øvelser af It beredskabsplanen både internt og i samarbejde med væsentlige leverandører.

Erfaringer fra beredskabstests og –øvelser skal indgå som inputgivende datakilder i It risikostyringen, herunder fastsættelsen og evalueringen af kontrol- og sikkerhedsforanstaltninger.

Der skal fastsættes regler for, hvordan beredskabshændelser, –tests og –øvelser afrapporteres.

Beredskabshændelser, –tests og –øvelser skal rapporteres til Jyske Banks bestyrelse og direktion.

Jyske Banks bestyrelse skal godkende beredskabsmålsætningen ved væsentlige ændringer, og minimum én gang årligt, så det sikres, at den er i overensstemmelse med koncernens risikoappetit.

10. *Kvalitetssikring*

Der skal udarbejdes procedurer, der sikrer tilstrækkelig kvalitetssikring af risikovurderinger, ændringer og den generelle It anvendelse.

Kvalitetssikringen skal dokumenteres og logges i et omfang, der muliggør opdagelse og fejlsøgning i forbindelse med adgangsstyring, ændringsstyring, risikovurderinger og sikkerhedsbrud.

11. *Brud på it sikkerhedspolitik og sikkerhedsregler*

I tilfælde af alvorlige brud på Sikkerhedspolitikken skal direktion og bestyrelse underrettes, og der skal reageres i forhold til omfanget af bruddet.

Forholdsregler og sanktionsmuligheder i tilfælde af brud på Sikkerhedspolitikken, samt underbyggende metodebeskrivelser, rammeværk, retningslinjer og forretningsgange skal nedfældes.

12. *Rapportering, kontrol og opfølgning*

Der skal implementeres og vedligeholdes operationelle- og verifikationskontroller, der sikrer, at It sikkerhedsniveauet er acceptabelt og modsvarer det aktuelle trussels- og It risikolandskab.

Der skal løbende ske opfølgning på, hvorvidt Sikkerhedspolitikken og dens underbyggende rammeværker, metodebeskrivelser og forretningsgange i tilstrækkelig grad sikrer, at det ønskede It sikkerhedsniveau opretholdes.

Bestyrelse og direktion skal løbende underrettes om It sikkerhedsniveauet i form af rapportering.

13. *Dispensationer fra Sikkerhedspolitikken*

Der skal forefindes en centraliseret og dokumenteret dispensationsstyringsproces, som sikrer struktureret og organiseret logning af dispensationer for Sikkerhedspolitikken, dens principper eller de underliggende retningslinjer.

Dispensationer skal tildeles på et risikobaseret grundlag, og altid være tidsbegrænsede.

Dispensation for sikkerhedspolitikken, dens principper eller underliggende retningslinjer kan bevilges af bestyrelsen, af direktionsmedlemmer og af afdelingsdirektøren for It sikkerhed og –risikostyring. Dispensationer skal dog altid godkendes af den eller de personer, der påtager sig ansvaret for risikoen forbundet med dispensationen.

It sikkerhed og –risikostyring er ansvarlig for behandlingen af dispensationsanmodninger, herunder at de indeholder en tilstrækkelig risikovurdering, som understøtter beslutning på et oplyst grundlag.

Rapportering omkring dispensationer varetages af It sikkerhed og –risikostyring.