Politik for It sikkerhed

Indhold

1. Formål og omfang 2
2. It-sikkerhedsniveau 2
3. Organisation og ansvar 2
4. It-risikostyring 3
5. Databeskyttelse 4
6. Outsourcing 6
7. Sikkerhedsprincipper 6
   7.1. Awareness 6
   7.2. Funktionsadskillelse 6
   7.3. Risikovurdering 6
   7.4. Beskyttelse af It aktiver 6
   7.5. Adgange til informationer og systemer 7
   7.6. Systemudvikling og vedligeholdelse af systemer 7
   7.7. Driftsafvikling 7
   7.8. Backup og sikkerhedskopiering 8
   7.9. Beredskab 8
   7.10. Kvalitetssikring 9
   7.11. Brud på it sikkerhedspolitik og sikkerhedsregler 9
   7.12. Rapportering, kontrol og opfølgning 9
   7.13. Dispensationer fra Sikkerhedspolitikken 9
8. Godkendelse af It sikkerhedspolitikken 10

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 tilstrækkeligt til at håndtere den aktuelle cybertrussel med elementer, der er "Best in class". Derudover skal sikkerhedsniveauet sikre, at de risici, som It anvendelsen medfører og forventes at medføre, er på et for koncernen acceptabelt niveau.
Fastsættelse af sikkerhedsniveauet skal modsvare udviklingen i trusselsniveauet på nationalt plan, baseres på risikovurderinger og efterleve sektorens lovgivning og krav.

It-sikkerhedsniveauet 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, retningslinjer og forretningsgange, som beskriver, hvorledes kravene heri operationaliseres.

Kravene, som er defineret i politikker, metodebeskrivelser, rammeværk, retningslinjer 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. 1st line er ansvarlige for at identificere, vurdere og håndtere risici, når de opdager dem.

- 2nd line udgøres primært af sikkerhedsafdelingen (IT-sikkerhed og –risikostyring), som overvåger it-sikkerhedsniveauet og risikoniveauet for it operationelle risici. 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.
Styring af It operationelle risici er underlagt Politik for operationel risikostyring, herunder risikomål og risikoappetit. Denne sikkerhedspolitik beskriver yderligere særlige principper og krav, der gør sig gældende for It risikostyring.

It risiko niveau

It risikoniveauet skal fastsættes og vedligeholdes på baggrund af risikovurderinger, der tager udgangspunkt i det omkringliggende trusselslandskab, regulatoriske krav, kontrol- og sikkerhedsforanstaltninger samt effektiviteten heraf, og andre relevante datainput, såsom dispensationer, revisionsanbefalinger, registrerede tab/fejl, driftshændelser, mv. Fastsættelse af It risikostyringsniveauet skal baseres på risikovurderinger og efterleve sektorens lovgivning og krav, og holdes op imod koncernens risikoappetit og risikotolerancer.

It risikovurderinger

Der skal foreligge risikovurderinger til grund for centrale vurderinger og beslutninger, der kan påvirke It anvendelsen i væsentlig grad, 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 information om faktiske fejl, problemer og svagheder.

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.

It risikostyringen skal baseres på en arbejdsproces, som tager højde for, at It risici er dynamiske og forandres i takt med ændringer til regulativer, trusselslandskab og It risikolandskab.

De forskellige faser i sådan en arbejdsproces for It risikostyringen skal tilgodese, at følgende risikostyringsaktiviteter er effektivt implementeret:

- Identify
  - Identifikation af risici skal ske i en åben risikokultur, hvor koncernens medarbejdere er aktive i at identificere og kommunikere risici. Risici identificeres på baggrund af medarbejderes viden og observationer samt inkludering af forskellige kilder, der kan give indsigt i risikolandskabet (eks. hændelser, sårbarheder, trusler mm.)
- Assess
  - Risici beskrives og vurderes ved hjælp af metoder og modeller der tydeliggør, hvorledes risici bedst håndteres. Eksempelvis ved tydelig angivelse af årsag, effekt, udløsende hændelse, kontroller og konsekvens.
- Review
  - For at sikre konsistens og et retvisende risikooverblik skal væsentlige risici igennem kvalitetsvurdering.
- Monitor
  - Væsentlige risici skal overvåges, herunder kontrolforanstaltninger og deres effektivitet. Registrering af risici og rapportering om status på risici skal ske ved passende frekvens, der tillader ledelsen at reagere rettidigt med henblik på styring af risikoniveauet.
- Retire
  - Risici, der ikke længere er relevante, slettes.

It risikolandskabet

It risikolandskabet er under konstant forandring, og en metode skal være implementeret, der tilsikrer, at der bliver taget stilling til væsentlige It risici, inden de realiseres, samt at metoden omfatter, at realiserede It risici identificeres, vurderes og håndteres effektivt, inden de materialiserer sig.

It risikolandskabet har høj kobling til forretningsprocesser, hvorfor væsentlige forretningsprocesser skal afdækkes for afhængigheder til It aktiver. It aktivernes tilstand (robusthed eller sårbarhed) kan påvirke forretningsprocessernes risikoprofil, hvorfor denne skal iagttages ved vurdering og styring af operationelle risici ud over it operationelle risici.

5. Databeskyttelse

Jyske Bank-koncernens aktiviteter forudsætter håndtering af personoplysninger, såvel almindelige oplysninger som følsomme oplysninger. Hovedparten af oplysningerne er almindelige oplysninger, men en stor del af disse er fortrolige oplysninger, som ikke skal uautoriserede personer eller offentligheden til kendskab. Af de personoplysninger, som Jyske Bank-koncernen behandler, hidrører den største del fra kunder, mens kun en lille del hidrører fra medarbejdere og andre grupper.

En behandling af ovenstående omfang er ofte forbundet med en høj iboende risiko for, at personoplysninger behandles forkert, hvilket kan føre til forkerte afgørelser, eller medfører at personoplysninger kan komme uvedkommende til kende og derved føre til en krænkelse af den registreredes rettigheder.

For at mindske den iboende høje risiko, relateret til håndteringen af de registrerede personoplysninger, skal følgende principper og foranstaltninger efterleves, når personoplysninger behandles:

- Data er til låns: Personoplysninger må ikke deles med uautoriserede personer, skal behandles med respekt, og skal afleveres tilbage i samme eller bedre stand, end den vi modtog dem i. Personoplysninger er således ikke noget, Jyske Bank-koncernen ejer, men noget vi har til låns fra kunderne/medarbejderne mfl.
- Risikobaseret tilgang: Enhver type af behandling af persondata skal risikovurderes med udgangspunkt i, hvilke risici behandlingen udsætter den registrerede for, og de tilstrækkelige og nødvendige sikkerhedsforanstaltninger samt forholdsregler skal etableres, således at disse risici nedbringes til et acceptabelt niveau. Hvor dette ikke er muligt, skal behandlingen ophøre.
- Awareness: Alle medarbejdere, der har kontakt med personoplysninger, skal modtage træning og instruktioner i, hvordan de skal behandle personoplysninger.
- Overblik: Der skal eksistere et overblik over, hvor i vores interne miljøer personoplysningerne er opbevaret, og til hvilke formål personoplysninger anvendes. Ligeledes skal der være et overblik over, hvilke databehandlere og underdatabehandlere der behandler personoplysninger på vegne af Jyske Bank-koncernen.
- Dataminimering: Der må kun indsamles og behandles den data, der er nødvendigt for at opfylde formålet med en given behandlingsaktivitet, ligesom det skal stå klart for den registrerede, hvorfor de konkrete oplysninger skal indsamles. Når personoplysningerne ikke længere er nødvendige, skal de anonymiseres eller slettes.
- Fortrolighed: Personoplysninger må kun kunne tilgås af autoriserede personer, og der skal opstilles tilstrækkelige og nødvendige sikkerhedsforanstaltninger, der sikrer, at uautoriserede personer ikke kan tilgå personoplysningerne. Dette er gældende såvel for interne som eksterne trusler.
- Integritet: Personoplysningerne skal være korrekte og ikke kunne modificeres uautoriserede personer.
- Tilgængelighed: Personoplysningerne skal være til rådighed til de formål, de er indsamlet til.
- Privacy by design: Alle systemer og processer, fremtidige som nuværende, skal indrettes/udfærdiges, så de efterlever disse principper og datatilsynets vejledninger.
- Kontrol over tillid: Det skal udføres effektive kontroller af
  - at medarbejderes omgang med personoplysninger efterlever ovenstående principper,
  - at systemer og processer bliver designet med fokus på privacy by design,
  - at leverandører efterlever samme principper og opretholder et tilstrækkeligt sikkerhedsniveau ift. beskyttelse af de personoplysninger, de behandler på vegne af Jyske Bank.
- Korrigerende foranstaltninger: Der skal opsættes de nødvendige og relevante foranstaltninger til at imødegå de brud på persondatasikkerheden, som uundgåeligt vil opstå.

Ovenstående principper skal implementeres i Jyske Banks-koncernens retningslinjer for efterlevelse af sikkerhedspolitikken.

6. 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.

7. 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:

7.1. Awareness

Løbende information og uddannelse til koncernens medarbejdere omkring it-sikkerhed og beskyttelse af persondata, skal sikre en bæredygtig sikkerhedskultur. Der skal foretages vurdering om målrettet It sikkerhedstræning for medarbejdere, som er i berøring med risikofyldte aktiviteter.

7.2. 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.

7.3. Risikovurdering

Der skal foreligge risikovurderinger til grund for centrale vurderinger og beslutninger, ligesom der skal foreligge risikovurderinger af væsentlige systemer for bankens drift. Nye systemer skal risikovurderes, før de sættes i produktion.

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.

7.4. Beskyttelse af It aktiver

It aktiver skal identificeres og beskyttes mod fysiske og logiske trusler i betryggende omfang. Dette gælder særligt for cybertrusler og trusler, som kan medføre fejl på It aktiverne, der giver betydelige konsekvenser for kunder, medarbejdere, samarbejdspartnere og øvrige personer, som er registreret i koncernen.

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.

7.5. Adgange til informationer og systemer

Adgangs rettigheder skal være begrundet i et arbejdsmæssigt behov, så vidt muligt være rollebaseret, og kunne 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.

7.6. Systemudvikling og vedligeholdelse af systemer

Der skal forefindes procedurer, der sikrer, at risici forbundet med udvikling, beskyttelse af personoplysninger, 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.

7.7. 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 sikkerhedspolitik angive krav, samt underbyggende metodebeskrivelser, politikker, retningslinjer og forretningsgange.

7.8. 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. Logisk og fysisk funktionsadskillelse skal sikres omkring backup miljøet.

7.9. 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 BCP'er, 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. Den aktuelle vurdering af koncernens anvendte datacentre vurderes som acceptabel til imødegåelse af hændelser, som kan opstå på baggrund af aktuelle infrastrukturelle, vejrmæssige, politiske og tekniske forhold.

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.

7.10. 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.

7.11. 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.

7.12. Rapportering, kontrol og opfølgning

Der skal implementeres og vedligeholdes operationelle- og verifikationskontroller i 1st og 2nd line, 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, retningslinjer 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.

7.13. Dispensationer fra Sikkerhedspolitikken

Der skal forefindes en centraliseret og dokumenteret dispensationsstyringsproces, som sikrer struktureret og organiseret logning af dispensationer fra 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.

8. Godkendelse af It sikkerhedspolitikken

Nærværende politik er modtaget af

Koncerndirektionen for Jyske Bank A/S
Silkeborg , den 10.12.2019

Anders Dam	Niels Erik Jakobsen
Per Skovhus	Peter Schleidt

Nærværende politik er godkendt af

Koncernbestyrelsen for Jyske Bank A/S
Silkeborg, den 10.12.2019

Sven Buhrkall	Kurt Bligaard Pedersen	Rina Asmussen
Philip Baruch	Jens A. Borup	Anker Laden-Andersen
Keld Norup	Per Schnack	
Johnny Christensen	Marianne Lillevang Jensen	Christina Lykke Munk