Politik for IKT-sikkerhed

Indhold

1. Formål og omfang

Formålet med denne Politik for IKT-sikkerhed (herefter benævnt sikkerhedspolitikken) er at sikre, at der implementeres og opretholdes et højt it-robusthedsniveau i Jyske Bank-koncernen (herefter benævnt koncernen), herunder at fastlægge principper og krav til it-sikkerhedsstyring, der sikrer, at it- sikkerhedsniveauet og den ønskede risikoprofil på it-området kan overholdes. Dette udmøntes i et stærkt cyberforsvar og robusthed i kritiske og vigtige funktioner.
Sikkerhedspolitikken skal hvert år fastlægges på baggrund af en aktuel risikovurdering, og kommunikeres ud til medarbejdere og relevante parter, herunder oploades på koncernens hjemmeside.
Sikkerhedspolitikken er gældende for alle ansatte i Jyske Bank, Jyske Realkredit, Jyske Invest og Jyske Finans, samt for alle tredjeparter, der har adgang til koncernens IKT-aktiver eller behandler koncernens information.

2. It-sikkerhedsniveau

2.1 Ambition

It-sikkerhedsniveauet skal fastsættes med udgangspunkt i koncernens ambition om at opnå og vedligeholde et digitalt operationelt robusthedsniveau, som er tilstrækkeligt til at håndtere den aktuelle cybertrussel med elementer, der er "Best in class". Derudover skal sikkerhedsniveauet til enhver tid være tilstrækkeligt til at sikre, at organisationen opererer inden for koncernens fastlagte risikoappetit for IKT-området.
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 IKT-systemer og it-anvendelse skal sikres en robusthed, som kan sikre stabil drift af koncernens kritiske funktioner og -forretningsprocesser samt sikre en cyberrobusthed, som er effektiv over for cyberangreb fra trusselsaktører, der arbejder med høj grad af organisering og sofistikerede angreb.

2.2 Cybersikkerhed og bæredygtighedsmål

Jyske Bank er bevidst om, at cybersikkerhed ikke kun er internt anliggende for at sikre stabil drift af koncernens kritiske funktioner og -forretningsprocesser, men med sin rolle som en af Danmarks største pengeinstitutter skal koncernens aktiviteter omkring cybersikkerhed også have en effekt på koncernens mål omkring bæredygtighed (ESG). Efterlevelse af kravene i denne sikkerhedspolitik bidrager til indfrielsen af disse mål, hvilket giver koncernens medarbejdere et supplerende incitament til at overholde sikkerhedspolitikken.

2.3 Sikkerhedsdokumentation

Sikkerhedspolitikken skal suppleres af dokumenterede indsatser, i en Digital Operationel

Robusthedsstrategi (DORS), som beskriver, hvorledes it-sikkerhedsniveauet skal opnås eller vedligeholdes. Derudover skal sikkerhedspolitikken uddybes i understøttende retningslinjer og forretningsgange, som beskriver, hvorledes kravene heri operationaliseres.

Kravene, som er defineret i retningslinjer og forretningsgange, skal til enhver tid efterleves. Afvigelser fra sikkerhedspolitikken skal risikovurderes. Er der tale om væsentlige afvigelser, som midlertidig accepteres, så skal der foreligge dispensationer fra sikkerhedspolitikken.

2.4 Sikkerhedspolitikkens godkendelse

Sikkerhedspolitikken skal godkendes af koncernbestyrelsen minimum én gang årligt eller ved væsentlige ændringer, som fordrer, at den revideres. Koncernbestyrelsen godkender ligeledes målsætninger, som koncerndirektionen skal sikre overholdt i forbindelse med den løbende opfølgning på, om sikkerhedspolitikken er overholdt.

3. Organisation og ansvar

Koncerndirektionen 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. Koncerndirektionen skal sikre en tilstrækkelig bemanding af sikkerhedsfunktionen, og at denne er bestående af kvalificerede medarbejdere, der afspejler koncernens behov.

Koncerndirektionen skal have minimum 1 direktionsmedlem med tilstrækkelig it-faglighed og kyndighed inden for it-sikkerhed til kunne sikre implementering og træffe nødvendige beslutninger omkring opretholdelsen af it-sikkerheden i koncernen.

Koncerndirektionen har udpeget en sikkerhedsansvarlig, herunder en It-sikkerhedsfunktion, og udstyret denne funktion til, uafhængigt af organisatorisk niveau, at håndhæve sikkerhedspolitikken.

Koncernen anvender en "3 Lines 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. I 1st line ligger tillige It-sikkerhedsfunktionen, som overvåger overholdelse af it-sikkerhedsniveauet, og at koncernen holder sig inden for risikotolerancen for it operationelle risici. 1st line udarbejder rapportering og anbefalinger omkring aktiviteter, der understøtter overholdelse af sikkerhedspolitikken.
- 2nd line udgøres af Risikofunktionen og Compliance funktionen. Risikofunktionen overvåger overholdelse af det samlede risikoniveau, hvori it operationelle risici også indgår. For overvågning af risikoniveau for it operationelle risici har

sikkerhedsfunktionen en delt organisatorisk reference til Risikofunktionen, som skal tilsikre, at risikokontroller kan defineres og udføres uafhængigt. Således kan Risikofunktionen udstikke krav til udførsel af risikokontroller til sikkerhedsfunktionen, som skal udføre disse uagtet organisatorisk tilhør i 1st line.
Compliance funktionen udfører også kontrolaktivitet i relation til lovgivning omkring it-sikkerhed. Compliance og Risikofunktionen skal udarbejde rapportering omkring it-sikkerhed iht. henholdsvis "Politik for compliancefunktionen I Jyske Bank-koncernen" og "Politik for operationel risikostyring i 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 koncernbestyrelsen.

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 risiko for koncernen, herunder risikomål og risikoappetit.

It-sikkerhedsfunktionen har ansvaret for at assistere organisationen med identifikation af it-risici, vurdering af sikkerhedsforanstaltninger og kontroller samt kvalitetssikring af de enkelte delelementer i it-risikovurderingerne, så de lever op til retningslinjerne beskrevet i Politik for operationel risiko for koncernen.

For at sikre størst mulig effektivitet og sammenhæng i arbejdet på tværs af områderne skal it-resort direktøren koordinere risikostyringsarbejdet løbende med den koncernrisikoansvarlige og den operationelle risikofunktion.

5. Databeskyttelse

Koncernen behandler i et stort omfang fortrolige oplysninger, herunder kunde- og personoplysninger. Størstedelen hidrører fra kunder, mens en mindre del relaterer til medarbejdere og andre grupper. Behandling af fortrolige oplysninger i en koncern af Jyske Banks størrelse medfører risiko for, at oplysninger behandles forkert, samt at oplysninger kan komme uautoriserede personer til kendskab og eventuelt blive udnyttet af disse.

For at mindske risikoen for, at fortrolige oplysninger behandles på en utilsigtet måde, arbejder koncernen ud fra grundlæggende principper for behandling og beskyttelse af fortrolige kunde- og personoplysninger:

- Lovlighed, rimelighed og gennemsigtighed: Behandlingen skal tage udgangspunkt i principper om lovlighed, rimelighed og gennemsigtighed
- Formålsbegrænsning: Særligt ved indsamling og behandling af personoplysninger skal det være klart, hvilke saglige formål oplysningerne skal anvendes til

- Dataminimering: Behandling og herunder opbevaring af særligt personoplysninger begrænses så vidt muligt til, hvad der er nødvendigt for at opfylde formålet med den pågældende behandling
- Rigtighed: Kunde- og personoplysninger ajourføres løbende, og urigtige oplysninger slettes eller berigtiges
- Opbevaringsbegrænsning: Særligt personoplysninger underlægges opbevaringsbegrænsning og opbevares alene, så længe de er nødvendige i forhold til de formål, som lå til grund for indsamling og behandling
- Integritet og fortrolighed: Fortrolige oplysninger, som behandles i koncernen, må ikke komme til uvedkommendes kendskab, gå tabt eller blive beskadiget. Gældende lovgivning vedrørende databeskyttelse og privacy indarbejdes i koncernens retningslinjer, forretningsgange og processer med udgangspunkt i en lav risiko-tolerance for brud på koncernens behandlingssikkerhed i tråd med den fastlagte ambition for koncernens digitale operationelle robusthedsniveau. Der sker løbende optimering af processer og sikkerhedsforanstaltninger med henblik på minimering af risiko.

It-sikkerhedsfunktionen og herunder DPO understøtter gennem underretning, rådgivning og overvågning koncernens overholdelse af forpligtelser i henhold til lovgivning vedrørende databeskyttelse og privacy.

6. Styring af tredjepartsrisici

Ved indgåelse af kontraktlige ordninger, med tredjepartsudbydere og deres eventuelle underleverandører, for brugen af IKT-tjenester skal it-sikkerhedsniveauet for koncernen opretholdes. Dette er ensbetydende med, at sikkerhedsprincipperne i sikkerhedspolitikken skal efterleves. Derudover skal der ved outsourcing vurderes, om målsætningerne for overholdelse af sikkerhedspolitikken kan imødekommes.
For tredjepartsudbydere af IKT-tjenester, der understøtter en kritisk eller vigtig funktion, skal denne overholde nyeste og højeste sikkerhedsstandarder.

Alle kontraktlige ordninger for brugen af IKT-tjenester skal registreres, herunder hvilke der understøtter kritiske eller vigtige funktioner.
Der skal udvises særlig opmærksomhed på styring af potentielle sikkerhedshændelser og -risici i relation til leverandører og tredjeparts IKT-ydelser, som kritiske eller vigtige funktioner er væsentligt afhængige af. Ligeledes skal leverandøren sikkerhedsmæssigt vurderes i forhold til ansvarlighed og evne til at opretholde det sikkerhedsniveau, som er vedtaget af koncernen. Risici og nødvendige foranstaltninger skal identificeres igennem en sikkerhedsvurdering og risikovurdering.

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 IKT-sikkerhed og digital operationel modstandsdygtighed samt 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, herunder tredjepartsudbydere. For at begrænse sikkerhedsmæssige risici, skal awareness information og awareness aktiviteter også muliggøre at forbrugere af koncernens digitale løsninger kan bruge disse trygt.

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.

Funktionsadskillelsen implementeres primært igennem organisatoriske strukturer og opdelte organisatoriske funktioner. Derudover sker implementering igennem adskillelse af adgange til systemer, der kan medføre store tab som følge af forkert anvendelse.

7.3. Risikovurdering og sikkerhedsvurdering

Der skal foreligge risikovurderinger til grund for centrale vurderinger og beslutninger, ligesom der skal foreligge risikovurderinger af IKT-systemer, der understøtter kritiske funktioner. Som en del af risikovurderingsaktiviteterne skal forretningsprocesser have gennemført konsekvensvurderinger, for at understøtte udarbejdelsen af koncernens risikoprofil og IKT-systemer skal tilstrækkeligt sårbarhedsvurderes. Dette gælder særlig IKT-systemer, der er nødvendige for understøttelsen af kritiske funktioner. Der skal være en tilstrækkeligt fuldstændig registrering af sammenhængen imellem kritiske funktioner, forretningsprocesser og understøttende IKT-systemer.
Nye IKT-systemer, som understøtter koncernens kritiske funktioner skal sikkerhedsvurderes, herunder 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 sårbarheder.

7.4. Beskyttelse af IKT-aktiver

IKT-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 IKT-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 IKT-aktiver beskyttes i betryggende omfang i forhold til koncernens risikoappetit, samt i henhold til lovgivning om databeskyttelse, hvor risici i forhold til datasubjektet (individet) skal vurderes.

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

IKT-aktiver skal være sikret af tilstrækkelige logiske og fysiske foranstaltninger.

7.5. Adgange til informationer og IKT-systemer

Adgangsrettigheder 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 IKT-aktiver og adgangene hertil.

7.6. Systemudvikling og vedligeholdelse af IKT-systemer

Der skal forefindes procedurer, der sikrer, at risici forbundet med udvikling, beskyttelse af personoplysninger, konfiguration og vedligeholdelse af nye og ændrede IKT-systemer identificeres, vurderes og håndteres.

Ændringsstyringsprocedurer skal foreligge i en sådan form, at væsentlige ændringer samt væsentlige risici, der er 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 som minimum udarbejdes og vedligeholdes dokumentation for alle IKT-systemer, der understøtter kritiske funktioner samt konfigurationer, og 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.

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 IKT-systemer og data.

Hyppigheden for sikkerhedskopiering og backup af IKT-systemer og data skal baseres på RTO og RPO krav samt dataenes klassifikation

Sikkerhedskopier og backups skal opbevares sikkert og være utilgængelige for uautoriserede personer og brugere. Logisk og fysisk funktionsadskillelse skal sikres omkring backup miljøet.

Backupmiljøet skal være robust over for cyberangreb, og skal overvåges og sikkerhedstestes med henblik på at opdage fejl og afvigelser.

7.9. Beredskab

Beredskabsmålsætningen skal som minimum fremgå i Politik for IKT-driftsstabilitet.

Beredskabsmålsætningen skal sætte mål for genetablering af normal drift i tilfælde af fejl, nedbrud, tab af data eller IKT-systemer, samt hel eller delvis ødelæggelse af bygninger, maskinel og kommunikationsveje.
Beredskabsmålsætningen skal tillige tage stilling til ekstreme men plausible scenarier.

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 kritiske funktioner i et acceptabelt omfang kan opretholdes i tilfælde af systemnedbrud, fejl og forstyrrelser i it-anvendelsen.

IKT-Systemer og data, der understøtter kritiske funktioner 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 IKT-relateret 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 IKT-relaterede 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 koncernens bestyrelser og direktioner.

Koncernbestyrelsen skal godkende Politik for IKT-driftsstabilitet ved væsentlige ændringer, og minimum én gang årligt, så det sikres, at den er i overensstemmelse med koncernens risikoappetit.

7.10. Sikkerhedstest

Med afsæt i de største risici for koncernen skal der udføres sikkerhedstest af de dertilhørende mest kritiske foranstaltninger. Omfang af test og hvilke foranstaltninger, der testes, skal prioriteres ud fra, hvordan koncernen har valgt at styre risici. Dermed menes, at hvis et risikoscenarie er kritisk afhængig af forebyggende foranstaltninger, så kan disse være vigtigere at teste fremfor korrigerende foranstaltninger.

Der skal som minimum udføres sikkerhedstest af alle IKT-systemer og -applikationer der understøtter kritiske eller vigtige funktioner mindst én gang om året, samt trusselsbaseret penetrationstest (TLPT-test) hvert 3. år. Omfang af testaktivitet kan variere med udgangspunkt i trusselsbillede og risikoniveau. Øvrige systemer skal testes inden for en 3-årig periode.

Idet koncernen anvender vigtige it-komponenter, som understøtter kritiske og vigtige funktioner, som er outsourcet, skal sikkerhedstest af disse også overvejes og sikres mulige at udføre, hvor det findes nødvendigt.

7.11. IKT-hændelses- og problemstyring

Effektive procedurer for IKT-relaterede hændelses- og problemstyring skal defineres og skal sikre, at it-risici og konsekvenser for som minimum kritiske funktioner identificeres, vurderes og håndteres, og indgår som datakilder i risikostyringsprocessen.
Alle IKT-relaterede hændelser skal registreres.
Effektiv kommunikation og rapportering omkring it-sikkerhedshændelser skal sikre hurtig og effektiv håndtering, således påvirkning af forretningsførelsen minimeres mest muligt.

Årsager til it-sikkerhedshændelser skal identificeres og fjernes, således gentagelser forhindres. Større IKT-relaterede hændelser skal rapporteres til Center for Cybersikkerhed og Finanstilsynet.

7.12. Logning og overvågning

Der skal udarbejdes procedurer for risikobaseret logning af brugeraktiviteter, undtagelser, fejl, IKT-relaterede hændelser og kritisk it-drift. Risikobaseret overvågning samt gennemgang af logs skal etableres.

Logning og overvågning af kritisk it-drift samt aktiviteter udført af privilegerede brugere skal prioriteres.

Løbende overvågning af kritiske forretningsfunktioner, it-administration, potentielle interne og eksterne trusler samt overvågning til afsløring af interne eller tredjeparters misbrug af adgange skal etableres.

7.13. IKT-sikkerhed i projektstyring

Koncernens metode for styring af it-projekter skal muliggøre, at risici kan identificeres og vurderes inden risiciene realiseres.
Herfor gælder, at for it-projekter, som kan medføre ændringer til risikoprofilen for koncernen, skal it- sikkerhedsfunktionen inddrages og konsulteres for at tilsikre at sikkerhedspolitikkens krav overholdes. Hvis it- projektet medfører realisering af høje risici skal risikofunktionen inddrages mhp. at vurdere om koncernens risikotolerance overskrides.

7.14. 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.

7.15. Brud på Politik for IKT-sikkerhed og sikkerhedsregler

I tilfælde af alvorlige brud på sikkerhedspolitikken skal koncernens direktioner og bestyrelser underrettes, og der skal reageres i forhold til omfanget af bruddet.

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

7.16. 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.

Koncernens bestyrelser og direktioner skal løbende underrettes om it-sikkerhedsniveauet i form af rapportering.

7.17. Dispensationer fra Politik for IKT-sikkerhed

Der skal forefindes en centraliseret og dokumenteret dispensationsstyringsproces, som sikrer struktureret og organiseret logning af dispensationer fra sikkerhedspolitikken, dens principper eller de underliggende retningslinjer og forretningsgange

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

Dispensation for sikkerhedspolitikken, dens principper eller underliggende retningslinjer kan bevilges af koncernbestyrelsen, og -direktion, samt af afdelingsdirektøren for sikkerhedsfunktionen. Dispensationer fra de underliggende forretningsgange kan bevilges af ledende medarbejdere i sikkerhedsfunktionen.

Dispensationer skal altid godkendes af den eller de personer, der påtager sig ansvaret for risikoen forbundet med dispensationen.

Sikkerhedsfunktionen 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 sikkerhedsfunktionen.

7.18. Anvendelse af kunstig intelligens (AI)

Koncernen skal anvende kunstig intelligens (AI) på en sikker og ansvarlig måde.

AI-systemer skal understøtte koncernens strategi uden at kompromittere informationssikkerhed, databeskyttelse, dataetik og kundetillid.

Der er anlagt en, i udgangspunktet, restriktiv tilgang til AI-udvikling i koncernen med fokus på ansvarlig implementering af ny teknologi i overensstemmelse me AI-forordningen samt et skærpet sikkerhedsmæssigt fokus på brugen af AI-løsninger i tilknytning til koncernens kritiske eller vigtige funktioner.

AI-systemer risikovurderes og klassificeres i overensstemmelse med gældende eksterne og interne krav, og der etableres passende tekniske og organisatoriske foranstaltninger til sikring af gennemsigtighed, robusthed og menneskelig kontrol. Brug af eksterne AI-tjenester overvåges og må kun ske, hvor det er forretningsmæssigt begrundet og sikkerhedsmæssigt forsvarligt, samt i overensstemmelse med koncernens retningslinjer for håndtering af tredjepartsrisici.

8. Godkendelse af Politik for IKT-sikkerhed

Nærværende politik er modtaget af

Koncerndirektionen for Jyske Bank A/S Silkeborg, 25.11.2025

Lars Mørch

Erik Gadeberg

Ingjerd Blekeli Spiten

Peter Schleidt

Jacob Gyntelberg

Nærværende politik er godkendt af

Koncernbestyrelsen for Jyske Bank A/S Silkeborg, den 25.11.2025

Kurt Bligaard Pedersen

Anker Laden-Andersen

Rina Asmussen

Lisbeth Holm

Birgitte Haurum

Bente Overgaard

Per Schnack

Glenn Söderholm

Henriette Hoffmann

Marianne Lillevang

Michael C. Mariegaard