Nykredit

# Politik for IT-Sikkerhed og Beredskab

Oktober 2024

| | | |
|---|---|---|
| Dokumentansvarlig: | STHY, IT Security & Privacy | |
| | | |
| Godkendt af, samt dato for godkendelse: | Bestyrelsen i: | |
| | Nykredit A/S | 05.12.2024 |
| | Nykredit Realkredit A/S | 05.12.2024 |
| | Totalkredit A/S | 04.11.2024 |
| | Nykredit Bank A/S | 04.11.2024 |
| | Nykredit Portefølje Administration A/S | 28.10.2024 |
| | Nykredit Leasing A/S | 05.11.2024 |
| | Nykredit Mægler A/S | 31.10.2024 |

| Dato | Forfatter | Version | Beskrivelse |
|---|---|---|---|
| 07-11-2019 | RE | 2.0 | Godkendt af ovenstående bestyrelser. |
| 21-02-2020 | RE | 2.0 | Opdateret med godkendelse hos Leasing og Mægler |
| 30-08-2020 | NAST | 2.1 | Detaljering omkring risikostyring, sikkerhedskrav og dispensationer. |
| 20-08-2021 | RE | 2.2 | Opdateret i henhold til ny lovgivning. Forhold omkring risikostyring er flyttet fra IT-Sikkerhedspolitikken til den nyoprettede Politik for it-risikostyring. |
| 08-09-2022 | STHY | 2.3 | Årlig opdatering – mindre justeringer |
| 29-09-2023 | MEKR | 2.4 | Årlig opdatering. Generelle justering, tilføjelser ift. DORA og nye *IT Security Requirements* (IT-Sikkerhedshåndbog). Derudover er it-risikostyring en del af denne politik og findes ikke længere som en separat politik. |
| 24-10-2023 | STHY | 2.5 | Opdateret med præcisering omkring rapportering til Risikokomiteen. |
| 26-10-2023 | STHY | 2.6 | Opdateret med præcisering vedr. halvårlig rapportering til Risikoudvalget. |
| 08-10-2024 | KLJ & DKBA | 2.7 | Opdateret i henhold til DORA-krav, herunder tilføjelse af beredskab i politikken |

# INDHOLDSFORTEGNELSE

# 1. BAGGRUND OG FORMÅL

Formålet med *Politik for it-sikkerhed og beredskab* er at fastlægge Nykredit-koncernens (herefter "Nykredit") overordnede krav til it-sikkerhed og beredskab ud fra den ønskede risikoprofil og det aktuelle trusselsniveau ved at håndtere it-risici i overensstemmelse med *Politik for ikke-finansielle risici og bestyrelsens retningslinjer for Nykredit Realkredit-koncernen*. Desuden er politikkens formål at realisere *Nykredits strategi for digital operationel robusthed og cybersikkerhed*.

Politikken er udformet således, at den imødegår de krav, som er fastlagt i *Forordning om digital operationel modstandsdygtighed i den finansielle sektor nr. 2022/2554 af 14. december 2022* (herefter "DORA") herunder regulatoriske tekniske standarder, der præciserer værktøjer, metoder, processer og politikker. Politikken skal ses i sammenhæng med *Direktionens retningslinjer for kontroller i Nykredit-koncernen*.

Politikken fastlægger de overordnede principper for Nykredits udøvelse af it-sikkerhed. Disse udformer sig som specifikke it-sikkerhedskrav i Nykredits *IT Security Requirements*, der udgør et vigtigt element i Nykredits interne kontrolmiljø. Derudover lægger politikken rammerne for Nykredits beredskab og dermed, hvordan man sikrer kontinuiteten og genoprettelsen af Nykredits kritiske forretningsområder i tilfælde af alvorlige driftsforstyrrelser. Udmøntningen heraf finder sted i form af Nykredits beredskabsplaner.

*Politik for it-sikkerhed og beredskab* opdateres og godkendes af koncernens bestyrelser minimum én gang årligt samt ved væsentlige ændringer.

## *1.1 Målsætninger*

Det er målsætningen at opretholde et tilstrækkeligt højt niveau af it-sikkerhed, der anerkender Nykredits samfundsansvar, og som sikrer fortrolighed, autenticitet, integritet og tilgængelighed af Nykredits it-aktiver, baseret på Nykredits vedtagne risikoappetit.

Det er desuden målsætningen at sikre kontinuiteten af kritiske forretningsområder i forbindelse med og efter alvorlige driftsforstyrrelser, og at forretningsmæssige tab begrænses til et minimum for Nykredit og Nykredits samarbejdspartnere.

### Konkrete målsætninger for beredskabet

For beredskabet har Nykredit endvidere fastsat en række konkrete målsætninger:

- Nykredit skal være i stand til at håndtere normale hændelser uden større driftsmæssig påvirkning.
- Nykredit skal ved større, kritiske beredskabshændelser være i stand til at etablere nøddrift, inden hændelsen får væsentlig indflydelse på Nykredits forretningsførelse. Konkrete målsætninger for etablering af nøddrift skal være defineret i de enkelte it-løsningers genopretningsplaner.
- Nykredit skal kunne vedligeholde nøddrift af kritiske forretningsprocesser, indtil man har opnået fuld genetablering af Nykredits it-løsninger.
- Nykredit skal kunne etablere nøddrift uden at være afhængig af enkeltsystemer.

# 2. ANVENDELSESOMRÅDER OG DEFINITIONER

## *2.1 Anvendelsesområder*

*Politik for it-sikkerhed og beredskab* gælder for hele Nykredit-koncernen med undtagelse af Sparinvest.

Politikken dækker alle organisatoriske, menneskelige, fysiske og tekniske forhold, som Nykredit anvender til at drive forretning, og gælder for alle medarbejdere og eksterne konsulenter i Nykredit.

Nykredit-koncernen benytter en række leverandører, som på grund af deres ydelser, kan have en indvirkning på it-sikkerhedsniveauet. Dette er i særdeleshed tilfældet med JN Data og BEC Financial Technologies (herefter "BEC"). Disse skal ligeledes leve op til Nykredits it-sikkerhedskrav. Således skal JN Data efterleve Nykredit-koncernens *IT Security Requirements* jf. it-hovedaftalen med JN Data. Ligeledes skal BEC gennem sine egne it-sikkerhedskrav opretholde et it-sikkerhedsniveau i overensstemmelse med Nykredit-

koncernens. For øvrige leverandører gælder det også, at disse – ud fra en risikobaseret tilgang – skal efterleve Nykredits krav til it-sikkerhed.

Bilag 1 indeholder et overblik over, hvor denne politik, *IT Security Requirements* og dispensationer gælder for Nykredit-koncernens selskaber samt JN Data og BEC.

Bilag 2 indeholder eksempler på it-sikkerhedsopgaver de enkelte selskaber i Nykredit-koncernen skal udføre.

### Undtagelser

*IT Security Requirements* gælder for hele Nykredit-koncernen med undtagelse af Nykredit Mægler. Da Nykredit Mæglers it-risikobillede adskiller sig væsentligt fra resten af Nykredit-koncernens, har Nykredit Mægler på baggrund af *IT Security Requirements* udarbejdet sine egne it-sikkerhedskrav.

For Nykredit Leasing er der indgået en aftale med IT Security & Privacy om, at efterlevelsen skal tilpasses ud fra Nykredit Leasings risikobillede og it-setup. I praksis betyder dette blandt andet, at hændelser skal videresendes til IT Security & Privacy, og dispensationer skal godkendes og følges af IT Security and Privacy. Derudover skal alle løsninger registres i koncernens fælles løsningsregister.

## *2.1 Definitioner*

**It-sikkerhed** indebærer beskyttelsen af it-aktiver med særlig fokus på beskyttelsen af disses fortrolighed, integritet, autenticitet og tilgængelighed.

**It-aktiver** forstås som alle former for it-relaterede ressourcer, som understøtter en forretning, og inkluderer både software, hardware og data.

**Fortrolighed** indebærer, at data er beskyttet mod uautoriseret adgang, anvendelse og offentliggørelse. Uvedkommende må således ikke få adgang til data, som kan misbruges til skade for Nykredit, Nykredits kunder, forretningsforbindelser eller medarbejdere.

**Integritet** indebærer, at datas konsistens, nøjagtighed og troværdighed opretholdes i hele datas livscyklus, herunder at data er beskyttet mod uautoriserede ændringer. For Nykredit gælder særligt beskyttelse mod manipulation i finansielle systemer.

**Autenticitet** indebærer, at data stammer fra sin oprindelige kilde. I Nykredit er autenticitetsbegrebet inkluderet i begrebet om integritet.

**Tilgængelighed** indebærer, at it-løsninger og data skal være tilgængelige for autoriseret anvendelse. Dette sikres ved rettidigt vedligehold, backup og beskyttelse af it-løsninger og data samt planlægning og test af reetablering.

**Beredskab** er, når forretningen i reaktion på en pludseligt opstået krise handler ud fra en række prædefinerede planer for at imødegå krisen på koncentreret, hurtig og effektiv vis.

**Business Impact Assessment** (herefter "BIA"), på dansk "forretningskonsekvensanalyse", er en analyse, som blandt andet vurderer de potentielle konsekvenser ved alvorlige driftsforstyrrelser eller datalæk. En BIA kan udarbejdes på forskellige niveauer herunder forretningsprocesser, forretningsfunktioner eller it-løsninger. BIA'er er medvirkende til at fastlægge forretningskritikalitet og danner bl.a. grundlag for krav til it-sikkerhed og it-drift samt udarbejdelse af beredskabsplaner.

**Beredskabsplaner** er de konkrete planer og procedurer, som udmønter beredskabet, og som tages i brug i forbindelse med krisesituationer og alvorlige driftsforstyrrelser. Beredskabsplaner kan dække over flere slags planer som f.eks. masternødplanen, forretningsnødplaner, genetableringsplaner m.m. De enkelte beredskabsplaner er beskrevet i nærmere detaljer i afsnit 5.2.

# 3. ORGANISERING OG ANSVAR

## 3.1 Bestyrelser og Direktioner

Bestyrelsen i Nykredit Realkredit A/S har det endelige ansvar for at sikre et tilfredsstillende it-sikkerhedsniveau til at håndtere identificerede it-risici, således at disse er indenfor den af bestyrelsen fastsatte risikoappetit, jf. *Politik for ikke-finansielle risici*. Bestyrelsen har desuden det endelige ansvar for at sikre et tilstrækkeligt beredskab.

Bestyrelsen i Nykredit Realkredit A/S og bestyrelserne i de enkelte datterselskaber bemyndiger deres direktioner til at sikre, at it-sikkerhed og beredskabet udmøntes i overensstemmelse med de i politikken nærmere fastsatte principper og rammer.

## 3.2 Risikokomiteen

Risikokomiteen varetager den løbende overvågning af it-risikoniveauet på vegne af Koncerndirektionen. Risikokomiteen modtager rapportering fra IT-Risikoudvalget, som består af Nykredits CIO, CISO, Head of "Infrastructure & Operations" og en forretningsrepræsentant, samt en observatør fra Risk & Conduct.

## 3.3 Beredskabskomiteen

Nykredits Beredskabskomite er den organisatoriske forankring af det udførende ansvar for beredskabet og koncernens samlede beredskabsplaner, jf. *Kommissorium for Nykredit Beredskabskomite*. Dette dækker såvel it- som forretningsberedskabet.

Beredskabskomiteen har ansvaret for at udarbejde og vedligeholde en særskilt masternødplan, jf. *Kommissorium for Nykredit Beredskabskomite*.

## 3.4 IT Security & Privacy

IT Security & Privacy er ansvarlig for Nykredits it-sikkerhedsarbejde og herigennem, at it-risici håndteres indenfor bestyrelsens risikoappetit. IT Security & Privacy udgør sammen med de enkelte forretningsenheder 1. forsvarslinje.

IT Security & Privacy skal med udgangspunkt i *Politik for it-sikkerhed og beredskab* definere et sikkerhedsniveau for anvendelsen af it i Nykredit. Dette udmøntes i *IT Security Requirements* og konkretiseres i forretningsgange mv. IT Security & Privacy skal overvåge og rapportere på efterlevelsen af det definerede it-sikkerhedsniveau i Nykredit og hos væsentlige it-leverandører.

IT Security & Privacy understøtter Nykredit med fortolkning, rådgivning og sparring vedrørende Nykredits *IT Security Requirements*.

## 3.5 Forretningsenheder

Forretningsenheder har det lokale ansvar for, at *Politik for it-sikkerhed og beredskab* og *IT Security Requirements* med tilhørende forretningsgange, regler mv. overholdes, samt at overholdelsen dokumenteres. Således udgør forretningsenhederne, sammen med IT Security & Privacy, 1. forsvarslinje. Det er desuden de enkelte enheders ansvar at udarbejde, vedligeholde og efterprøve forretningsnødplaner for deres respektive forretningsområder i overensstemmelse med krav i *IT Security Requirements*. Den forretningsansvarlige chef (på niveau 2) har det overordnede risikoansvar, er ansvarlig for at godkende planerne og mindst én gang årligt foranstalte eftersyn (test, afprøvning mv.) af disse med efterfølgende opfølgningsaktiviteter og godkendelse.

I forbindelse med krisesituationer er det den enkelte forretningsansvarlige chef, der har de sædvanlige ledelsesbeføjelser.

## 3.6 Uafhængige kontrolfunktioner og Intern Revision

Risk & Conduct overvåger og kontrollerer, at it-risici og øvrige ikke-finansielle risici styres tilstrækkeligt, mens Compliance overvåger og kontrollerer compliance-risici på it-området. Disse udgør således 2. forsvarslinje.

Intern revision reviderer det interne kontrolsystem og vurderer, om det er i overensstemmelse med det niveau, bestyrelsen har udstukket. Intern Revision udgør dermed 3. forsvarslinje og refererer direkte til bestyrelsen.

# 4. PRINCIPPER FOR IT-SIKKERHED

Politikkens målsætninger og dertilhørende principper for it-sikkerhed skal udmøntes i it-sikkerhedskrav, som er de sikkerhedsforanstaltninger og andre risikoreducerende tiltag, der blandt andet skal beskytte Nykredits it-aktiver mod tab af fortrolighed, autenticitet, integritet og tilgængelighed. Kravene skal beskrives i *IT Security Requirements*. For hvert it-sikkerhedskrav skal der angives fordeling af roller og ansvar ved brug af RACI-modellen[1].

Arbejdet med it-sikkerhed skal tage udgangspunkt i ISO 27000-serien, herunder principperne for ledelsessystemet i 27001, sikkerhedsforanstaltningerne i 27002:2022 og privatlivsbeskyttelse i 27701:2019. En *Statement of Applicability* (SoA) skal udarbejdes for at dokumentere til- og fravalget af sikkerhedsforanstaltninger.

Principperne for it-sikkerhed fordeles på fire hovedområder. Disse hovedområders væsentlige emner bliver beskrevet nedenfor.

## *4.1 Organisatoriske kontrolforanstaltninger*

### Forvaltning af it-aktiver

It-aktiver og it-aktivers livscyklus skal overvåges og styres centralt. It-aktiver skal have et passende it-sikkerhedsniveau i forhold til disses risici. It-aktiver må ikke idriftsættes uden forudgående godkendelse fra IT Security & Privacy.

It-aktiver, herunder legacy-it-løsninger, skal registreres i en central fortegnelse, der indeholder relevante oplysninger såsom indbyrdes afhængigheder og genopretningskrav.

### Dataklassifikation

Data skal differentieres afhængig af disses beskyttelsesbehov. I Nykredit klassificeres data i tre overordnede kategorier, som beskrevet i tabellen nedenfor.

*Table 1: Nykredits dataklassifikationssystem.*

| Klassifikation | Beskrivelse |
|---|---|
| **Offentligt tilgængelig data** | Denne kategori indeholder oplysninger, som er offentligt tilgængelige, offentlige personoplysninger undtaget. |
| **Intern data** | Denne kategori indeholder forretningsmæssig oplysninger, som frit kan tilgås inden for Nykredit-koncernen. |
| **Fortrolig data** | Denne kategori indeholder forretningsmæssigt fortrolige oplysninger om Nykredit-koncernen og dens forretningsførelse, samt alle typer af personoplysninger som defineret i databeskyttelsesforordningen. |

Kategorierne er yderligere specificeret i *IT Security Requirements.* Hvis data ikke er klassificeret, skal det antages, at de er klassificeret som *Intern data*.

### Adgangsstyring

It-aktiver skal have en passende grad af adgangsstyring. Adgangsrettigheder skal i alle tilfælde tildeles på baggrund af need to know-, need to use- og least privileged-princippet, og skal godkendes ud fra principperne for funktionsadskillelse. Adgangsrettigheder skal gennemgås i en passende frekvens.

### It-projektstyring

It-projekter skal styres efter en formaliseret metode, der sikrer en effektiv og sikker gennemførsel. It-sikkerhed skal være en integreret del af Nykredits projektstyringsmetode.

### Anskaffelse, udvikling og vedligeholdelse af it-løsninger

Anskaffelse, udvikling og vedligeholdelse af it-løsninger skal styres efter en formaliseret

[1] RACI (**R**esponsible, **A**ccountable, **C**onsulted, **I**nformed) er en matrice, der benyttes til at fordele ansvarsområder.

metode, der sikrer, at it-løsningen lever op til den aftalte kvalitet. It-sikkerhed og kvalitetssikring skal være en integreret del af Nykredits udviklingsmetode, der yderligere skal indeholde krav til ændringsstyring og test.

### Styring af it-relaterede hændelser

Nykredit skal etablere og kommunikere en proces for opdagelse, styring, indberetning og reaktion på it-hændelser herunder rolle- og ansvarsfordeling.

Processen skal sikre detektion og overvågning af cybertrusler og anormale aktiviteter internt i Nykredit og hos leverandører, samt sikre, at der sker løbende læring og evaluering ved afsluttede hændelsesforløb.

### Informationsudveksling og vidensdeling

Nykredit skal deltage i relevante fora med henblik på at forbedre den digitale operationelle robusthed og sikre udveksling af efterretninger, viden og information om it-risiko, it-sikkerhed, trusler og hændelser.

## *4.2 Menneskelige kontrolforanstaltninger*

### Menneskelige ressourcer

Der skal være en klar angivelse af it-sikkerhedsopgaver og -ansvar, samt hvilke medarbejdere eller enheder disse tildeles.

Alle medarbejdere skal forstå og anerkende deres it-sikkerhedsmæssige ansvar i deres daglige funktion. Det indebærer herunder at efterleve retningslinjer på området og undergå relevant uddannelse i nødvendigt omfang og frekvens.

Medarbejdere, som bryder med *Politik for it-sikkerhed og beredskab* eller *IT Security Requirements*, kan blive udsat for disciplinære konsekvenser i overensstemmelse med Nykredits regler på det personaleadministrative område.

## *4.3 Fysiske kontrolforanstaltninger*

### Skærm- og skrivebordspolitik

Med henblik på at bevare fortrolighed, integritet, autenticitet og tilgængelighed af Nykredits data skal brug af arbejdsstationer følge ”clear screen”- og ”clear desk”-principper. Dette skal være gældende både på og uden for Nykredits lokationer.

## *4.4 Tekniske kontrolforanstaltninger*

### Styring af it-operationer

It-sikkerhed skal være en integreret del af anvendelse, overvågning, kontrol og genopretning af Nykredits systemer og data.

### Styring af netsikkerhed

Der skal implementeres sikkerhedsmekanismer, som sikrer fortroligheden, integriteten, autenticiteten og tilgængeligheden af netværk og netværksenheder i Nykredit.

Der skal ske passende segmentering af netværk og filtrering af trafik mellem disse, hvor det er muligt. Segmentering skal bl.a. adskille interne og eksterne zoner, forskellige forretningsområder og udviklings- og test-miljøer.

Der skal ske passende styring af adgang til eksterne webressourcer for at reducere eksponering for skadeligt eller ondartet indhold.

### Sikring af oplysninger, som er under overførsel

Med henblik på at bevare fortrolighed, integritet, autenticitet og tilgængelighed af Nykredits data skal der implementeres tilstrækkelige sikkerhedsmekanismer til at beskytte data under overførsel (*data in transit*). Mekanismerne skal afspejle behovet for beskyttelse af data ud fra datas kritikalitet.

Hvor det er muligt, skal forsøg på at flytte eller lække fortrolig data detekteres og undersøges.

### Kryptering og kryptografiske kontrolforanstaltninger

It-aktiver skal benytte en passende grad af kryptografi, der afspejler aktivernes vurderede risikoniveau. Hvor kryptografi ikke er muligt, skal andre sikkerhedsforanstaltninger implementeres for at sikre et passende it-sikkerhedsniveau.

Krypteringsnøgler skal forvaltes igennem deres livscyklus.

### Sikkerhedskopiering

Med henblik på at muliggøre effektiv genetablering af Nykredits it-løsninger og applikationer og sikre forretningskontinuiteten i forbindelse med alvorlige driftsforstyrrelser skal der ske sikkerhedskopiering af Nykredits it-aktiver i passende omfang og efter en fastlagt frekvens. Det er hertil essentielt, at Nykredit har allokeret tilstrækkelige redundante ressourcer og kapacitet til at sikre, at forretningen kan fungere så upåvirket som muligt ifm. alvorlige hændelser.

For at sikre at det forventede behov for genetablering kan imødekommes, skal sikkerhedskopiering af systemer og data testes i passende interval og omfang og som minimum på årlig basis.

## *4.5 Dispensationer*

I det omfang de udstukne bestemmelser i indeværende *Politik for it-sikkerhed og beredskab* eller *IT Security Requirements* ikke kan efterleves, eller at risikoen ikke er proportionel med de økonomiske eller forretningsmæssige konsekvenser, kan IT Security & Privacy på vegne af bestyrelserne og direktionerne dispensere fra politikken eller *IT Security Requirements*, såfremt det fortsat vil være i overensstemmelse med it-sikkerhedsmålsætningen. Der kan ikke dispenseres fra krav, der vil medføre manglende efterlevelse af gældende lovgivning eller risici udenfor risikoappetitten.

Dispensationer fra krav skal risikovurderes, præsenteres for direktion og bestyrelse i form af en årsrapport og revurderes i en passende frekvens. Herudover skal dispensationer indgå i det løbende it-risikobillede. En dispensation med risiko af kritisk karakter skal således direkte afspejles i risikorapporteringen fra IT Security & Privacy til Risikokomiteen.

Forud for en dispensation skal der foreligge en skriftlig ansøgning, som har til formål at dokumentere alle afgørelser. Dispensationer skal være tidsbegrænsede. IT Security & Privacy skal i et passende interval kontrollere, at tidsfrister er overholdt.

# 5. BEREDSKABET

## *5.1 Business Impact Assessment (BIA)*

Nykredits beredskabsstyring skal være baseret på en omfattende forretningskonsekvensanalyse/Business Impact Assessment (BIA). BIA'en skal kortlægge og vurdere kritikaliteten af Nykredits forretningsprocesser- og funktioner, it-løsninger, tredjepartsafhængigheder og it-aktiver med dertilhørende afhængigheder mhp. at disse kan prioriteres efter en risikobaseret tilgang. Beskyttelsen af Nykredits IT-aktiver og -services skal baseres på BIA'ens resultater mhp. at sikre disses redundans.

BIA'en skal opdateres hvert år samt i forbindelse med væsentlige retslige ændringer, organisatoriske ændringer, ændringer i trusselsbilledet eller ændringer i Nykredits risikoprofil.

## *5.2 Beredskabsplaner*

*Politik for it-sikkerhed og beredskab* udmøntes i en masternødplan, forretningsnødplaner, genetableringsplaner, IT-beredskabsplaner og krisekommunikationsplaner.

**Masternødplanen** er Beredskabskomiteens overordnede plan i en beredskabssituation. Masternødplanen skal dække organisering, interessenter, aktiviteter og kommunikation i en beredskabssituation for Nykredit. Masternødplanen skal opdateres regelmæssigt samt i forlængelse af efterprøvninger og efter aktivering.

**Forretningsnødplaner** dækker alle manuelle procedurer og forretningsgange på forretningsområder, herunder aftaler med eksterne partnere, der skal sikre, at Nykredit kan fungere på et acceptabelt niveau i tilfælde af katastrofer, dvs. hvordan forretningsområderne vil videreføre deres forretning, mens it-miljøet bliver genetableret. Forretningsnødplaner er udarbejdet på baggrund af forretningskonsekvensanalyser (BIA'er) på det respektive forretningsområde og skal udarbejdes for alle kritiske forretningsprocesser. Ansvaret for forretningsnødplanerne er placeret hos koncernens forretningsansvarlige for de enkelte forretningsområder.

**Genetableringsplaner for it-løsninger og applikationer** beskriver de tekniske tiltag og forudsætninger for genetablering af de enkelte komponenter i løsninger. Genetableringsplanerne skal udvikles med øje for deres betydning for kritiske forretningsfunktioner og -processer og for deres eksponering for cyber-trusler. Alle it-løsninger, som vurderes som værende forretningskritiske, skal have en genetableringsplan, og disse skal have defineret genopretningsmål, som svarer til løsningens kritikalitet.

**IT-beredskabsplaner** dækker hele Nykredits it-anvendelse, uanset om disse er outsourcede, herunder reetablering af it-driften i tilfælde af katastrofer. Nykredits it-beredskabsplaner skal været prioriterede ud fra en risikobaseret tilgang med udgangspunkt i BIA'en.

**Krisekommunikationsplaner** sikrer en behørig formidling af større hændelser, nedbrud og trusler overfor kunder, klienter, samarbejdspartnere samt den øvrige offentlighed. Krisekommunikationsplanerne skal udarbejdes med reference til Nykredits generelle kommunikationspolitik, som bl.a. definerer kommunikative roller og ansvar i forbindelse med alvorlige driftsforstyrrelser.

### *5.3 Tests af beredskabet*

Nykredits beredskab skal testes på årlig basis eller i forbindelse med større ændringer i forretningskritiske it-løsninger. Dette er for at sikre, at beredskabet og tilhørende beredskabsplaner er tidssvarende og opdaterede, og at Nykredit grundlæggende udviser den nødvendige modstandsdygtighed til at sikre den fortsatte drift af forretningens kritiske funktioner ved alvorlige driftsforstyrrelser. Testene skal tage udgangspunkt i den udarbejdede BIA.

Resultaterne fra beredskabstests skal dokumenteres mhp. videre læring, og eventuelle mangler i beredskabet skal behandles og rapporteres videre til Nykredits bestyrelser.

## 6. OVERVÅGNING OG UDVIKLING

### *6.1 Overvågning*

Som beskrevet ovenfor, foretages der overvågning på forskellige niveauer i Nykredit-koncernen.

IT Security & Privacy overvåger it-sikkerhedsniveauet på tværs af koncernen med henblik på at identificere undtagelser til gennemførslen af *Politik for it-sikkerhed og beredskab* og *IT Security Requirements* og for at sikre at it-sikkerhedsniveauet bevares til trods for disse undtagelser. Derudover overvåges it- og compliance-risici i 2. forsvarslinje af hhv. Risk & Conduct og Compliance, mens Intern Revision reviderer de interne kontroller ved tilsyn. Beredskabskomitteen er desuden ansvarlig for løbende at overvåge beredskabsindsatsen for at sikre beredskabets effektivitet samt overensstemmelse med relevante lovkrav.

Overvågningen omfatter bl.a. sporing og rapportering på i forvejen fastsatte mål, dokumentation og analyse af hændelser mhp. at lære og identificere forbedringspotentiale samt regelmæssige tilsyn for at sikre overholdelse af interne politikker og lovkrav.

It-sikkerhedsniveauet skal vurderes ved brug af forskellige metoder for efterprøvelse, herunder både audits og tekniske test. Metoderne skal variere, således at Nykredit overvåger it-sikkerhedsniveauet i bredden og dybden.

### *6.2 Opdateringer*

*Politik for it-sikkerhed og beredskab* og dertilhørende forretningsgange og beredskabsplaner

skal gennemgås og opdateres på årlig basis eller i tilfælde af væsentlige hændelser. Opdateringen kan bl.a. ske på baggrund af lovmæssige ændringer, teknologiske, organisatoriske eller forretningsmæssige ændringer eller efter input fra medarbejdere, samarbejdspartnere eller tilsynsmyndigheder.

### *6.3 Løbende udvikling*

Beskyttelsen af Nykredits it-aktiver skal løbende udvikles på baggrund af læring fra driftsforstyrrelser eller andre sikkerhedshændelser, best practice i den finansielle sektor, læring fra globale hændelser samt deltagelse i fagrelevante fora.

## 7. RAPPORTERING

IT Security & Privacy skal løbende rapportere til It-risikoudvalget, Risikokomiteen, Risikoudvalget samt direktioner og bestyrelse jf. nedenstående tabel.

IT Security & Privacy rapporterer kvartalsvis til It-risikoudvalget. It-risikoudvalget har jf. kommissoriet for Risikokomiteen fået delegeret ansvaret for overvågning og styring af Nykredits it-risici herunder koncernens it-sikkerhed. It-risikoudvalget foretager halvårligt rapportering til Risikokomiteen med hovedområderne fra It-risikoudvalget. Derudover kan der, baseret på en konkret vurdering fra IT Security & Privacy, foretages særskilt rapportering på it-risici til direktioner eller i særlige tilfælde bestyrelser.

Endvidere skal IT Security & Privacy rapportere halvårligt til Risikoudvalget, og årligt til de enkelte bestyrelser. Denne rapportering skal indeholde en overordnet vurdering af it-risikobilledet, koncernens it-sikkerhed og beredskabsindsatsen.

Slutteligt skal IT Security & Privacy rapportere fire gange årligt angående it-risikoscenarier til Risk & Conduct, som har ansvaret for, at risici bliver rapporteret videre til direktioner og bestyrelser. I indberetningen til Risk & Conduct skal de identificerede it-risici beskrives, kategoriseres og risikovurderes. Endvidere skal det angives, hvilke kontrolforanstaltninger og øvrige risikoreducerende foranstaltninger, der er implementeret for at nedbringe risikoen og sikre, at risikoen er indenfor Nykredits risikoappetit. Rapportering skal ske på selskabsniveau.

IT Security & Privacy er desuden forpligtet til løbende at rapportere ved væsentlige hændelser til direktioner og Nykredits bestyrelser, hvis relevant. Nykredit skal desuden rapportere til relevante tilsynsmyndigheder ved større hændelser og nedbrud.

| Rapportering | Frekvens | Modtager |
|---|---|---|
| Sikkerhedsrapporten<br>(Status på it-risici, it-sikkerhed og beredskab) | Kvartalsvis | It-risikoudvalget |
| It-risikoscenarier i Risikorapporten | Kvartalsvist | Risikokomiteen |
| It-risikobilledet | Halvårligt | Risikokomiteen |
| Halvårsrapport<br>Relevante emner og status på it-risici, it-sikkerhed, it-drift og beredskab | Halvårligt | Risikokomiteen<br>(Direktioner)<br>Risikoudvalget<br>Bestyrelser |

## 8. IKRAFTTRÆDELSE

*Politik for it-sikkerhed og beredskab* træder i kraft på tidspunktet for bestyrelsernes godkendelse.

## Bilag 1: Oversigt over politikkens anvendelsesområder

| | Nykredit Realkredit A/S | Nykredit Bank A/S | Totalkredit A/S | Nykredit Portefølje Administration A/S | Nykredit Leasing A/S | Nykredit Mægler A/S | Sparinvest S.A. | JN Data A/S | BEC Financial Technologies a.m.b.a. |
|---|---|---|---|---|---|---|---|---|---|
| **Politik for it-sikkerhed og beredskab** | X | X | X | X | X | X | | | |
| **IT Security Requirements** | X | X | X | X | X | | X | X | (X) |
| **Dispensationer** | X | X | X | X | X | X | X | X | |

## Bilag 2: It-sikkerhedsopgaver i Nykredit-koncernens selskaber

| Opgave | Nykredit Realkredit A/S | Nykredit Bank A/S | Totalkredit A/S | Nykredit Portefølje Administration A/S | Nykredit Leasing A/S | Nykredit Mægler A/S | Sparinvest S.A. | JN Data A/S | BEC Financial Technologies a.m.b.a. |
|---|---|---|---|---|---|---|---|---|---|
| **Gennemføre it-sikkerheds-vurderinger** | X | X | X | X | X | | X | | |
| **Registrere løsninger i SEACOR** | X | X | X | X | X | X | X | | |
| **Indberette hændelser** | X | X | X | X | X | X | X | X | X |
| **Underlagt test af it-sikkerhed (inspektioner m.m.)** | X | X | X | X | X | X | | X | X |