Nykredit

Totalkredit

Politik for IT-Sikkerhed

December 2022

Dokumentansvarlig:	STHY, IT Security	
Godkendt af, samt dato for godkendelse:	Bestyrelsen i:	
	Nykredit A/S	02.11.2022
	Nykredit Realkredit A/S	02.11.2022
	Totalkredit A/S	31.10.2022
	Nykredit Bank A/S	31.10.2022
	Nykredit Portefølje Administration A/S	25.10.2022

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

INDHOLDSFORTEGNELSE

1. FORMÅL 4
2. OMFANG 4
3. OVERORDNET IT-SIKKERHEDSMÅLSÆTNING 4
4. LEDELSES- OG STYRINGSMODEL 5
4.1. ORGANISERING OG ANSVAR 5
6. KLASSIFIKATION AF INFORMATIONER 6
7. SIKKERHEDSKRAV 7
7.1. DISPENSATIONER 9
8. HÆNDELSES – OG BEREDSKABSSTYRING 9
8.1. BEREDSKABSMÅLSÆTNING 9

1. FORMÅL

Formålet med Politik for IT-Sikkerhed er at fastlægge Nykredit-koncernens overordnede krav til it-sikkerhed ud fra den ønskede risikoprofil og det aktuelle trusselsniveau. Dette skal sikre Nykredits strategiske mål for anvendelse af elektronisk informationsbehandling, herunder overholdelse af lovmæssige og regulative krav. Derudover fastlægger Politik for IT-SIkkerhed rammerne for cybersikkerhed med henblik på at sikre Nykredit mod cyberangreb.

Ansvarsplacering, retningslinjer, procedurer, risikovurdering og beredskabsplaner for it-sikkerhed er således emner, der reguleres under denne overordnede politik.

2. OMFANG

Politik for IT-Sikkerhed dækker alle tekniske, processuelle og menneskelige forhold, der kan påvirke de services og systemer, som Nykredit anvender til elektronisk informationsbehandling herunder også de services og systemer, der leveres af underleverandører.

Politikken gælder for alle medarbejdere og eksterne konsulenter i Nykredit og er samtidig rammen for den it-sikkerhedsleverance, som Nykredit forventer fra leverandører af it-ydelser.

I denne politik og tilhørende håndbøger, retningslinjer, arbejdsgangsbeskrivelser eller tilsvarende dokumenter, forstås it-sikkerhed som følgende:

Sikring af alle it-informationsaktiver, der indgår i eller bidrager til behandlingen af digitale informationer. Sikringen sker vha. teknologi, mennesker og processer, hvor alle tre elementer er vigtige for at opnå den tilstrækkelige og mest effektive sikkerhed.

3. OVERORDNET IT-SIKKERHEDSMÅLSÆTNING

Nykredit er af Finanstilsynet udpeget, som operatør af væsentlige tjenester, og it-sikkerhedsmålsætningen er fastlagt på den baggrund.

Der skal leveres en effektiv, pålidelig og sikker leverance af it-ydelser, idet anvendelsen af it er et bærende element i udøvelsen af Nykredits forretning. Nykredit ønsker at følge best practice indenfor sin branche sammenholdt med en tilgang, hvor sikkerhedstiltag afvejes i forhold til omkostninger og sikkerhedsmæssig værdi for Nykredit.

Nykredits it-miljø skal være tilstrækkeligt sikkert til at modstå alment kendte cyberangreb, og være tilstrækkeligt robust, så systemer kan genskabes indenfor rammerne fastsat i beredskabsmålsætningen. Derudover må kompromitteringen af et enkelt it-system eller computer ikke sætte Nykredits samlede it-miljø i fare.

Niveauet for it-sikkerhed skal til stadighed være afstemt med direktionens forventninger og behov for at sikre, at niveauet ligger indenfor bestyrelsens definerede risikoappetit. Dette sker gennem sikkerhedsvurderinger, hvori der fastlægges krav til Fortrolighed, Integritet og Tilgængelighed. Herudover skal der kontinuerligt foretages vurdering og kontrol af de implementerede sikkerhedstiltag, sammenholdt med sektorstandarder og vurdering af det aktuelle trusselsbillede.

It-sikkerhed kan traditionelt opdeles i nedenstående områder:

Fortrolighed
Ved fortrolighed forstås, at data er beskyttet mod uautoriseret adgang, anvendelse og offentliggørelse. Det er sikret, at uvedkommende ikke kan få adgang til data, som kan misbruges til skade for Nykredit, Nykredits kunder, forretningsforbindelser eller medarbejdere.

Integritet
Ved integritet forstås, 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.

Tilgængelighed
Ved tilgængelighed forstås, at systemer og data skal være tilgængelige for autoriseret anvendelse. Dette sikres ved rettidig vedligehold, backup og beskyttelse af systemer og data samt planlægning og test af reetablering.

4. LEDELSES- OG STYRINGSMODEL

Til at sikre den tilstrækkelige ledelsesinvolvering i it-sikkerheden har Nykredit etableret en ledelses- og styringsmodel, der er forankret i bestyrelsen, direktionen og den øvrige organisation.

Rammerne for ledelses- og styringsmodellen er fastlagt i Politik for IT-Risikostyring, Politik for IT-Sikkerhed, IT-Sikkerhedshåndbogen, forretningsgange, organisatoriske beslutningsgange og aktiviteter, som understøtter det it-sikkerhedsniveau og de ambitioner, der er udstukket af bestyrelsen i denne politik.

Politik for IT-Risikostyring fastlægger den overordnede risikoappetit på it-området, samt definerer hvorledes it-risici identificeres, styres og rapporteres.
Politik for IT-Sikkerhed definerer de overordnede rammer for it-sikkerhed med udgangspunkt i den fastsatte risikoappetit. IT-Sikkerhedshåndbogen (retningslinje) opstiller konkrete it-sikkerhedskrav, der sikrer at it-sikkerheden er indenfor de rammer, der er defineret i Politik for IT-Sikkerhed. Herunder følger forretningsgange, organisatoriske beslutningsgange og aktiviteter, heriblandt rapportering på risici og andre relevante forhold.

4.1. ORGANISERING OG ANSVAR

De pågældende bestyrelser og direktioner i alle selskaber i Nykredit-koncernen har det overordnede ansvar for it-sikkerheden i de enkelte selskaber.

Risikokomiteen varetager den løbende overvågning af it-sikkerhedstyringen og it-risikoniveauet på vegne af Koncerndirektionen.

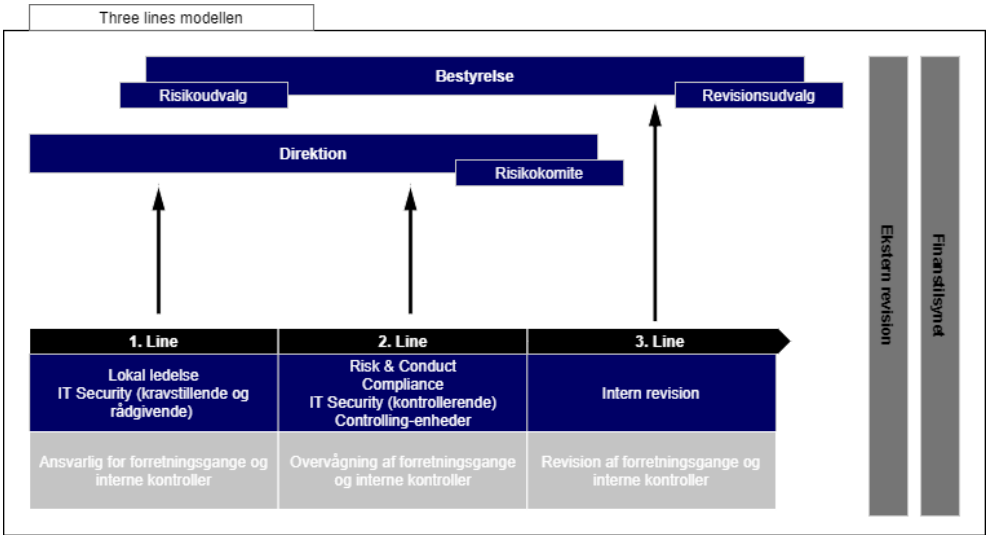
Sikkerhedsudvalget, bestående af CIO, CISO, Head of IT Delivery og Head of Infrastructure & Operations, behandler tekniske it-sikkerhedsmæssige udfordringer. IT-Sikkerhedsudvalget er underlagt og rapporterer til Risikokomiteen.

IT Security har ansvaret for udarbejdelse og vedligeholdelse af Politik for IT-Risikostyring, Politik for IT-Sikkerhed og tilhørende sikkerhedskrav baseret på en risikovurdering af koncernens it-anvendelse og har i den forbindelse en aktiv, kontrollerende og rapporterende rolle med hensyn til overholdelsen af IT-Sikkerhedspolitikken i hele Nykredit med reference til direktionerne i koncernen.
Politik for IT-Sikkerhed opdateres og godkendes af bestyrelser en gang årligt eller ved væsentlige ændringer.

Efterlevelse af Politik for IT-Sikkerhed sikres af de enkelte direktioner vha. specifikation af konkrete krav i IT-Sikkerhedshåndbogen, der opdateres og godkendes af de respektive direktioner en gang årligt eller ved væsentlige ændringer.

De enkelte organisatoriske enheder i koncernen har det løbende, lokale ansvar for, at Politik for IT-Sikkerhed og IT-Sikkerhedshåndbogen med tilhørende forretningsgange, regler mv. overholdes samt at overholdelsen dokumenteres. For at sikre forankringen af dette ansvar skal alle it-løsninger have en entydig ansvarlig, som er registreret en centralt sted.

Ansvaret er opstillet i Figur 1 og ansvaret i de enkelte linjer er detaljeret nedenfor.



Figur 1- 3 Lines of defense

1. Line – Lokal ledelse, IT Security
Nykredit arbejder med et princip om decentralt ansvar. Det betyder, at linjeledelsen har det nære ansvar for, at it-sikkerhedsniveauet fastholdes gennem de daglige forretningsgange. Det er således linjeledelsens ansvar at afdække hvilke it-sikkerhedskrav, der falder indenfor eget ansvarsområde og efterleve disse, samt efterfølgende gennemføre opfølgning på efterlevelsens effektivitet ved at implementere relevante kontroller.
Tilsvarende gennemfører relevante procesejere opfølgning på, at deres processer efterleves og udfører dermed 1. line kontrol i forhold til brugerne af processerne.
IT Security fastlægger de overordnede krav til kontroller i 1. line og understøtter organisationen med fortolkning og sparring vedrørende Nykredits it-sikkerhedskrav.

2. Line – Compliance, Risikostyring, IT Security
IT Security overvåger efterlevelsen af de udstukne sikkerhedskrav. Efterlevelsen rapporteres til den risikoansvarlige, risikomitéen, direktion og bestyrelse.

3. Line - Intern revision

Intern revision udgør det sidste lag i modellen. Intern revision reviderer det interne kontrolsystem og vurderer, om det er i overensstemmelse med det niveau, bestyrelsen har udstukket. Intern revision refererer direkte til bestyrelsen.

5. KLASSIFIKATION AF INFORMATIONER

I Nykredit klassificeres information i tre overordnede kategorier: *offentligt tilgængelig information, intern information* og *fortrolig information*.

KLASSIFIKATION	BESKRIVELSE
Offentligt tilgængelig information	Denne kategori indeholder oplysninger, som er offentligt tilgængelige, offentlige persondata undtaget.
Intern information	Denne kategori indeholder forretningsmæssig information, som frit kan tilgås inden for Nykredit koncernen.
Fortrolig information	Denne kategori indeholder forretningsmæssigt fortrolig information om Nykredit-koncernen og dens forretningsførelse samt alle typer af personoplysninger, som defineret i gældende persondata-lovgivning.

Hver kategori har differentierede krav til fortrolighed, og alle sikkerhedskrav i *IT-Sikkerhedspolitikken*, *IT-Sikkerhedshåndbogen* og *Den Blå Folder* tager udgangspunkt i disse kategorier. Kategorierne er yderligere specificeret i *IT-Sikkerhedshåndbogen*.

Hvis informationer ikke er klassificeret skal det antages, at de er klassificeret som "*Intern Information*".

6. SIKKERHEDSKRAV

Sikkerhedskravene er de sikkerhedsforanstaltninger og kontroller, der skal beskytte Nykredits it-informationsaktiver.

Nykredit arbejder ud fra de sikkerhedskrav, der er defineret i ISO27001, Anneks A. Nykredit sikrer, at ISO27001 kravenes til- og fravalg begrundes. Ansvaret herfor er placeret i IT Security.

Sikkerhedskravene designes med det formål at maksimere beskyttelsen af it-informationsaktiverne, at øge medarbejdernes effektivitet, hvor det er muligt, sikre efterlevelse af lovkrav relatere til it-anvendelse samt undgå unødvendige omkostninger. Ved at arbejde ud fra best pratice-kravene i ISO27001:2017 sikres professionalismen, kvaliteten og styrken i Nykredits it-sikkerhedsleverancer og –løsninger.

De enkelte sikkerhedskrav er beskrevet i Nykredits IT-Sikkerhedshåndbog med tilhørende underbilag. I forlængelse heraf udarbejder og dokumenterer de enkelte områder og afdelinger i Nykredit de relevante forretningsgange, metoder, vejledninger, tjeklister mv.

Sikkerhedskravene i IT-Sikkerhedshåndbogen er fordelt på følgende hovedområder (baseret på ISO27001, Anneks A):

- ***Informationssikkerhedspolitikker*** *(kapitel 5)*
  Alle dokumenter, der indeholder regler, grænser eller guidelines relateret til it-sikkerhed, skal følge de generelle krav til sådanne i Nykredit. De skal derudover have en ejer, som skal sikre, at de bliver opdateret mindst en gang om året eller ved større ændringer.

- ***Organisering af informationssikkerhed*** *(kapitel 6)*
  It-arbejdet er organiseret under Digital, Change & IT under COO-området. Herunder er udvikling og drift som udgangspunkt adskilt i seperate organisatoriske enheder. Der anvendes dog også agile udviklingsmetoder, herunder *DevOps og SecDevOps*, hvor udvikling og drift pågår i samme organisatoriske enhed. Digital, Change & IT leverer it-understøttelse til alle Nykredits organisatoriske enheders forretningsførelse, hvor der er behov herfor.

  Der skal være passende funktionsadskillelse indenfor brugeradministration, review og godkendelse, log information, backup data samt it-udvikling og drift. Afdelingslederen er ansvarlig for ovenstående bliver overholdt og kontrolleret mindst årligt eller ved signifikante ændringer.

  IT Security skal altid konsulteres ved projekter der indeholder risici relateret til it-sikkerhed og når nye it-løsninger bliver designet, anskaffet og/eller implementeret.

- ***Medarbejdersikkerhed*** *(kapitel 7)*
  Alle medarbejdere og konsulenter skal have læst og forstået relevant it-sikkerhedsinformation samt følge denne.

- ***Styring af aktiver*** *(kapitel 8)*
  Alle løsninger i Nykredit skal registreres centralt med en entydig ejer. Alle løsninger bør desuden have et passende niveau af it-sikkerhed ud fra en risikobaseret tilgang.

  Alle løsninger skal benyttes efter hensigten samt, hvor det giver mening, tilbageleveres til Nykredit ved endt brug.

  Løsninger må ikke idriftssættes uden forudgående godkendelse fra IT Security.

- ***Adgangsstyring*** *(kapitel 9)*
  Løsninger bør have en passende grad af adgangsstyring og følge relevante

forretningsgange for området. Alle adgange skal gennemgås mindst én gang om året af nærmeste leder og hvor muligt også af løsningens ejer.

- ***Kryptografi*** *(kapitel 10)*
  Nykredits løsninger bør alle benytte en passende grad af kryptografi. Det er ejeren af den enkelte løsnings ansvar at sikre dette og indhente godkendelse fra IT Security.

- ***Fysisk- og miljøsikring*** *(kapitel 11)*
  Procurement, Facility Management og IT er overordnet ansvarlige for et passende niveau af fysisk- og miljøsikring. Dog har alle brugere af løsninger et ansvar for, at disse benyttes på den foreskrevne sikre måde.

- ***Driftssikkerhed - heriblandt: Driftsafvikling, logning, overvågning samt sikkerhedskopiering*** *(kapitel 12)*
  Alle løsninger skal have relevant driftsdokumentation, der også skal beskrive den benyttede logning, backup, overvågning og sikkerhedskopiering, som skal leve op til IT-Sikkerhedshåndbogen og relevante forretningsgange. Løsningens ejer er ansvarlig for dette.

  Der skal foretages periodiske risikovurderinger af løsninger, hvor løsningens kritikalitet afgør hvor ofte risikovurderingen skal opdateres.

- ***Kommunikationssikkerhed*** *(kapitel 13)*
  Løsningers ejere skal sikre, at kommunikationsvejene har en passende grad af beskyttelse og lever op til interne retningslinjer fra IT Security.

- ***Anskaffelse, udvikling og vedligeholdelse af systemer, herunder kvalitetssikring*** *(kapitel 14)*
  Nykredits udviklingsmetoder skal understøtte, at systemerne lever op til den aftalte kvalitet og it-sikkerhed. Udvikling, anskaffelse og igangsætning af systemer skal ske efter en godkendt og beskrevet metode, der blandt andet skal indeholde krav til ændringsstyring, test og kvalitetssikring. Kvalitetssikring skal være en integreret del af Nykredits udviklingsmetoder.

- ***Leverandørforhold*** *(kapitel 15)*
  Der skal indgås skriftlige aftaler med eksterne samarbejdspartnere, og de krav, der stilles til leverandørerne, skal baseres på Nykredits forretningsmæssige behov. For at stille de mest effektive sikkerhedsmæssige krav, skal kritiske risici i forhold til leverandøren og leverancen identificeres. Kravene skal herefter formuleres, så de imødegår de identificerede kritiske risici. I den forbindelse skal Nykredit sikre, at gældende lovgivning og sektorkrav er overholdt.

  Efter aftalens indgåelse skal ydelser fra leverandører af forretningskritiske eller følsomme leverancer regelmæssigt overvåges og vurderes med henblik på at evaluere sikkerhedsniveauet i leverancerne. Ansvaret herfor er placeret hos kontraktejeren med praktisk bistand fra IT Security.

- Hvis leverandøren behandler personoplysninger på vegne af Nykredit, skal der indgås
- en databehandleraftale, som følger interne retningslinjer for disse. Hvis der er tvivl om, hvorvidt der foreligger en databehandlerkonstruktion, skal Persondatajura kontaktes.

  Det skal vurderes, om der i leverandøraftalen skal stilles krav om revisorerklæring fra leverandøren, eksempelvis 3402- eller 3000-erklæring etc.

- ***Styring af informationssikkerhedsbrud*** *(kapitel 16)*
  Se afsnit om hændelses- og beredskabsstyring.

- ***Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring*** *(kapitel 17)*
  Se afsnit om hændelses- og beredskabsstyring.

- ***Overensstemmelse, herunder overholdelse af relevant lovgivning*** *(kapitel 18)*
  Løsningens ejer er ansvarlige for, at den lever op til gældende lovgivning og politiker

samt heraf afledte forretningsgange, retningslinjer m.m.

Som opfølgning på om sikkerhedskravene anvendes og fungerer effektivt, gennemføres kontrol af implementering og effektivitet lokalt. IT Security og Compliance udfører 2nd line kontrol ud fra en risikobaseret tilgang. I det omfang kontrolmålinger viser, at sikkerhedskrav ikke fungerer så effektivt som forventet, iværksættes den eller de indsatser, der vurderes relevant for at effektivisere sikkerhedskravet.

IT Security gennemfører løbende og minimum årligt kontrol af efterlevelse af IT-Sikkerhedspolitikken for alle selskaber, den er gældende for, i Nykredit-koncernen, herunder væsentlige underleverandører. Resultatet rapporteres til bestyrelserne i de respektive selskaber.

6.1. DISPENSATIONER

I det omfang de udstukne bestemmelser i Politik for IT-isikostyring, Politik for IT-Sikkerhed eller IT-Sikkerhedshåndbogen ikke kan efterleves, eller at risikoen ikke er proportional med de økonomiske eller forretningsmæssige konsekvenser, kan IT Security på vegne af bestyrelsen og direktionen dispensere fra kravene såfremt det fortsat vil være i overensstemmelse med it-sikkerhedsmålsætningen.
Dispensationer fra krav skal risikovurderes, præsenteres for direktion og bestyrelse i form af en årsrapport og revurderes minimum årligt. Herudover skal dispensationer indgå i det løbende it-risikobillede. En dispensation med risiko af kritisk karakter skal således direkte afspejles risikorapporteringen fra IT Security til Risikokomiteen.

Forud for en dispensation skal der foreligge en skriftlig ansøgning til IT Security, som skal dokumentere alle afgørelser. Alle dispensationer er gyldige i maksimum 12 måneder og IT Security skal minimum én gang i kvartalet kontrollere at tidsfrister er overholdt.

Der kan aldrig gives dispensation for at bryde relevant lovgivning såsom GDPR, ej heller kan der gives dispensationer hvor risikoen forbundet hermed vurderes til at være *kritisk.*

7. HÆNDELSES – OG BEREDSKABSSTYRING

Opdages brud på Politik for IT-Sikkerhed, IT-Sikkerhedshåndbogen, eller forhold der i øvrigt kan true it-sikkerheden hos Nykredit håndteres dette gennem den etablerede proces for it-sikkerhedshændelser af IT Security.

Medarbejdere, som bryder IT-Sikkerhedspolitikken eller IT-Sikkerhedshåndbogen, kan blive udsat for disciplinære forholdsregler i overensstemmelse med Nykredits regler på det personaleadministrative område.

Nykredits Beredskabskomité er den organisatoriske forankring af det udførende ansvar for efterlevelse af IT-Sikkerhedspolitikkens regler i relation til beredskabet og koncernens samlede beredskabsplaner, dvs. dækkende såvel it-aspekterne som forretningsaspekterne.

Det medlem af koncerndirektionen, som er ansvarlig for it-området i koncernen, er formand for komitéen.

Beredskabskomitéen har ansvaret for udmøntningen af koncernens beredskabsplaner dækkende såvel it-aspekterne som forretningsaspekterne og udgør tillige krisestaben i tilfælde af katastrofer, større uheld mv.

I tilfælde af tidskritiske it-sikkerhedsmæssige forhold bemyndiges CISO'en til undtagelsesvis at standse forretningsaktiviteter midlertidigt, indtil Beredskabskomitéen kan træffe beslutning på området, såfremt CISO'en vurderer at det er nødvendigt for at beskytte Nykredits overordnede it-drift.

7.1. BEREDSKABSMÅLSÆTNING

Den overordnede målsætning for beredskabet er, at en beredskabssituation vedrørende Nykredits it-understøttelse ikke må medføre væsentlige forretningsmæssige tab eller medføre, at Nykredits fremtidige forretningsførelse kommer i fare. Som følge heraf, skal der

implementeres flercenterdrift for alle forretningskritiske systemer.

Koncernens beredskabsplaner dokumenteres i:

- Masternødplanen, der er Beredskabskomitéens overordnede plan i en beredskabssituation. Planen dækker organisering, interessanter, aktiviteter og kommunikation i en beredskabssituation.
- Forretningsnødplaner dækker alle manuelle procedurer og forretningsgange, inkl. aftaler med eksterne partnere, der skal sikre, at Nykredit kan fungere på et acceptabelt niveau i tilfælde af katastrofer, og er ansvarsplaceret hos koncernens forretningsansvarlige for de enkelte forretningsområder.
- Genetableringsplaner for systemer og applikationer, der beskriver de tekniske tiltag og forudsætninger for genetablerng af de enkelte komponenter i løsninger.
- IT-beredskabsplaner, som dækker hele Nykredits it-anvendelse, uanset om disse er outsourcede, herunder retablering af it-driften i tilfælde af katastrofer, og er ansvarsplaceret i Infrastructure & Operations.
- Det er den enkelte forretningsansvarlige chef, som har ansvaret for, at der for egne ansvarsområder udarbejdes forretningsnødplaner svarende til de udstukne retningslinjer, som godkender disse og mindst én gang årligt foranstalter eftersyn (test, afprøvning mv.) heraf med efterfølgende opfølgningsaktiviteter og godkendelse.
- I forbindelse med krisesituationer er det den enkelte forretningsansvarlige chef, der har de sædvanlige ledelsesbeføjelser og ansvar for medarbejdere i forbindelse med gennemførelse af forretningsaktiviteterne støttet af forretningsnødplanerne, som har ledelsesansvaret for de forretningsaktiviteter, der skal bringe situationen tilbage til de normale driftsforhold.

Med hensyn til udenlandske enheder skal der også etableres både forretningsmæssigt og it-mæssigt beredskab, jf. ovenstående. Aktiviteterne er underlagt Beredskabskomitéen.