Politik

Emne: **IT-sikkerhedspolitik for Spar Nord Bank A/S**

Version: **3.4, af 1. juli 2022**

spar nord

Indhold

IT-sikkerhedspolitikken er struktureret således at afsnit 6-18 er passer med ISO27002-standardens afsnit indeholdende sikkerhedsforanstaltninger for at forenkle sammenhængen til best practice. Øvrige afsnit 1-5 og 19-24 er refereret til ISO27001.

0. Læsevejledning

IT-sikkerhedspolitikken er opdelt i følgende struktur:

1 Den overordnede IT-sikkerhedspolitik (dette dokument) beskriver målsætninger, rammer, hovedkrav, risikostyring og -håndtering, hovedroller/-ansvar/-beføjelser, sikkerhedshændelser/-afvigelser, dispensationer, ledelsesrapportering samt vedligeholdelse.

IT-sikkerhedspolitikken er struktureret således at afsnit 6-18 passer med ISO27002[1]-standardens afsnit indeholdende sikkerhedsforanstaltninger for at forenkle sammenhængen til best practice. Øvrige afsnit 1-5 og 19-24 er refereret til ISO27001[2].

IT-sikkerhedspolitikken vil ændre sig i takt med, at der sker større ændringer i kravene enten fra eksterne eller interne kilder.

2 IT-sikkerhedsregler udarbejdes som særskilte dokumenter, som understøtning af politikken. En oversigt over de til enhver tid godkendte og gældende IT-sikkerhedsregler findes sammen med nærværende IT-sikkerhedspolitik på Intranettet.

IT-sikkerhedsregler ændres, enten når opfattelsen af "best practice" udvikler sig, eller når der er konkrete krav fra ledelsen, lovgivning, tilsyn eller lignende. Forventede ændringer kunne være tiltag, som forbedrer IT-sikkerheden. Reduktioner i IT-sikkerhedsregler vil også kunne forekomme, hvis det overholder kravene til styring og forretningsmæssig accept af risici.

3 Detaljerede instrukser for håndtering af IT-sikkerhed i hverdagen, henhører under respektive ansvarsområder. Ansvar for instrukser for håndtering af data beror hos dataejer, ansvar for instrukser for håndtering af systemer beror hos systemejer og ansvar for processer beror hos procesejer.

Ændringer i instrukser kan forventes, hvis en forretningsproces ændres, ved nye versioner eller hvis der ibrugtages funktionalitet, der ikke tidligere har været aktiveret.

Det er dataejers/systemejers/procesejers ansvar, at ændringer i instruks er risikovurderet. Hvis risikovurdering viser en forøget risiko i forhold til eksisterende risikovurdering, skal dette afspejles i bankens risikoregister.

1. Introduktion

1.1 Indledning

Digitale og fysiske informationer samt IT-systemer er vitale for moderne bankdrift. Udvikling af basis banksystemer er outsourcet til BEC. Udvikling og drift af et antal kritiske og værdiskabende systemer varetages af Spar Nord selv, eks. økonomisystemer, udlandssystemer og risikostyring.

Det er derfor en forretningsmæssig forudsætning, at vi er i stand til at holde vores IT-systemer kørende og vore kommunikationslinjer åbne, samtidig med, at vi beskytter vore kunders og bankens vitale informationer mod uvedkommendes indsigt.

Da informationer og IT-systemer er nødvendige og livsvigtige for Spar Nord, har IT-sikkerheden en afgørende betydning for bankens troværdighed og fortsatte eksistens. Det rette sikkerhedsniveau for Spar Nord tilvejebringes ved en løbende vurdering af trusselsbilledet og iværksættelse af nødvendige sikringstiltag.

1 ISO 27002 giver anbefalinger om bedste praksis om kontrol af informationssikkerhed til brug for dem, der er ansvarlige for at initiere, implementere eller vedligeholde ISMS (Information Security Management Systems).

2 ISO 27001 opstiller blandt andet krav til risikostyring, dokumentation af processer samt fordeling af roller og ansvar for informationssikkerhed.

Spar Nord overholder gældende lovgivning, samtidig med, at det er væsentligt, at forretningens løbende drift og overlevelse sikres.

Et højt sikkerhedsniveau understøtter Spar Nords værdier om ansvarlighed, og at Spar Nord leverer kvalitet gennem en sikker service til kunder og samarbejdspartnere.

1.2 Gyldighedsområde for IT-sikkerhed (ISO27001:2017, afsnit 4)

IT-sikkerhedspolitikken omfatter Spar Nord Bank A/S, tilhørende datterselskaber samt enhver samarbejdspartner, herunder leverandør, serviceleverandører og outsourcing partner, som tilgår Spar Nord Bank A/S netværk eller data, enten internt eller eksternt.

Politikken er understøttet af sikkerhedsregler, som er målrettet til intern anvendelse. I forhold til 3. parter, anvendes sikkerhedsregler og instrukser, som er relevante for konteksten. Sikkerhedsreglerne beskriver de minimumskrav der skal efterleves, for at være compliant med den aktuelle politik.

De væsentligste elementer der indgår i den samlede IT-sikkerhed er:

- Ledelsesbekendtgørelsens bilag 5
- IT-sikkerhedspolitikken
- IT-risikostyringspolitik
- IT-politik
- Datagovernancepolitik
- Databeskyttelsespolitik
- Outsourcingpolitik
- BIA (Business Impact Analysis)
- IT-trussels- og -risikoregistrering
- Eskaleringsmodel (fremgår af afsnit 17. IT-sikkerhedskrav til beredskab)
- IT-Beredskabsplan
    - Målsætning
    - Kommunikationsmodel
    - Beredskab
- Regler og procedurer for IT-sikkerhed
- Risikovurderinger
- Backup
- IT-drift, IT-hændelser (Incident- og problemmanagement) og ændringsstyring (change management og idriftsætning)
- IT-dokumentation
- IT-udvikling og -test
- Serviceniveauaftaler (SLA'er)
- Roller (Systemejer/Dataejer/Brugersystemansvarlig (BSA))
- IT-projektstyring
- IT-anskaffelser og IT-aktiver (logiske, fysiske, ressourcer og data)
- Forretningskritikalitet f.s.v.a. IT-systemer, -processer og data
- Medarbejderes daglige håndtering af informationer og data
- IT-sikkerhedsuddannelse og -awareness

IT-sikkerhedspolitikken omfatter enhver form for IT-anvendelse, herunder hardware, systemer og data m.m. IT-sikkerhedspolitikken dækker også fysiske data. Outsourcede IT-aktiviteter skal være omfattet af politikken ved skriftlige aftaler.

Regler og procedurer for IT-sikkerhed udformes, så de opfylder lovgivningens og forretningens krav til IT-sikkerhed. Regler og procedurer tilrettelægges så de giver størst effektivitet og mindst administration i den daglige drift.

Almindelig god etik og moral skal efterleves ved anvendelse af systemerne.

Politik og regler skal være udformet, kommunikeret og tilgængelige, så alle medarbejdere har mulighed for at efterleve disse, og ikke uberettiget bliver gjort ansvarlige for hændelser ved fornuftig omgang med data, systemer og udstyr, ligesom ansvaret for de enkelte elementer i indholdet skal være fastlagt.

2. Målsætning (ISO27001:2017, afsnit 5.1.a og 6.2)

IT-sikkerhedspolitikken har, som målsætning, at Spar Nord, med udgangspunkt i bankens risikoprofil og i kraft af en effektiv og sikker databehandling, kan bidrage til den forretningsmæssige strategi og samtidig fremstå som en professionel, troværdig og respekteret bank, samarbejdspartner og arbejdsgiver.

Bankens bestyrelse ønsker med IT-sikkerhedspolitikken at understøtte, at der af ledelsen træffes foranstaltninger, der effektivt og tilpasset bankens forhold, tilgodeser de fire overordnede sikkerhedskrav:

- **Fortrolighed**, der skal sikre, at informationer beskyttes mod utilsigtet offentliggørelse. Informationer og systemer skal sikres mod uautoriseret adgang og anvendelse samt øvrige krav, der stilles af vores kunder, myndigheder og bankens ledelse.
- **Integritet**, der skal sikre, at informationer er korrekte, nøjagtige og fuldstændige, og at anvendte IT-systemer fungerer korrekt og som forventeligt.
- **Tilgængelighed**, der skal sikre, at informationer og IT-faciliteter er tilgængelige, når organisationen har brug for det.
- **Lovgivning og sektorkrav**, der sikrer, at Spar Nord opfylder gældende lovgivning dækkende IT-sikkerhed og IT-risici

IT-sikkerhedspolitikken skal også sikre en medarbejderansvarlighed i relation til sikkerheden omkring virksomhedens informationer og IT-systemer. IT-sikkerhedspolitikken, understøttende regler for IT-sikkerhed samt instrukser vejleder medarbejdere i, hvordan sikkerhedsmæssige hændelser kan minimeres eller helt undgås.

3. IT-sikkerhed (ISO27001:2017, afsnit 6.1)

3.1 Sikkerhedsniveau

Udgangspunktet er, at IT-sikkerhedspolitikken følger principperne for god IT-skik, gældende lovgivning, og hvad der anses for at være "best practice". Sidstnævnte er udmøntet ved at benytte ISO27001/ISO27002 som rammeværktøj.

Sikkerhedsniveauet er fastlagt ud fra Spar Nord Bank A/S' metode for risikovurdering, baseret på ledelsens fastsatte niveau for risikovillighed/-tolerance indenfor de tilladte, lovmæssige rammer.

IT-Sikkerhed skal implementere et passende antal kontroller, som har til formål at følge op og rapportere på overholdelse af bankens IT-sikkerhedspolitik.

Der gennemføres auditeringer af sikkerhedsniveauet af intern og ekstern revision ud fra revisionens krav.

3.2 Vores holdninger og principper

IT-sikkerhedspolitikken indebærer en afvejning imellem forhold, der kan være modstridende. IT-sikkerhedstiltag kan medføre højere omkostninger end ønsket, og medføre, at brugervenligheden må vige.

Ledelsens holdning er dog, at IT-sikkerhed er afgørende vigtig for Spar Nord Bank A/S, og ledelsen tillader ikke, at forretningsmæssige ønsker eller dispositioner sker på bekostning af IT-sikkerheden. CISO'en afgør om beslutninger sker på bekostning af IT-sikkerheden og skal afrapportere tilfælde til ledelsen, som afvigelser fra IT-sikkerhedspolitikken. CISO'en skal i rapporteringer til ledelsen medtage beslutninger, som har været tæt på at være brud på IT-sikkerhedspolitikken, hvis CISO'en skønner stigende tendens til grænsetilfælde.

I det følgende uddybes i hovedtræk, hvordan ledelsens holdninger og principper er udmøntet i sikkerhedsregler.

Fortrolige data
Spar Nord behandler og opbevarer sine data med henblik på at opretholde fortrolighed i forhold til information, som måtte kræve fortrolighed, herunder forretningskritisk information. Dette gælder for ansattes omgang med data, og i forbindelse med anvendelse af IT-systemer. Der anvendes kun IT-systemer til behandling og opbevaring af data, som Spar Nord aktivt har valgt at tage i anvendelse. Beslutningen skal til enhver tid være understøttet af en risikovurdering af det pågældende IT-system.

Ansatte må ikke anvende private webmailtjenester eller private internetbaserede tjenester (fildelingstjenester, sociale netværk o.lign.) til distribution, opbevaring af Spar Nord information. Dette må udelukkende forekomme i interne mails i bankens godkendte mailsystem.

Det godkendte mailsystem skal anvende sikre kommunikationsmetoder i forbindelse med eksterne fortrolige data, eksempelvis følsom fondsbørs–korrespondance med erhvervskunder, og tilsvarende iagttage Spar Nords GDPR-regler for kommunikation med private kunder, offentlige myndigheder el.lign.

Systemkvalitet
IT-systemer der indgår og anvendes af banken, skal i hele ibrugtagningsperioden opfylde bankens acceptkrav for drift og forvaltning, herunder efterlevelsen af krav for tekniske sikkerhedsforanstalt-ninger samt for driftsafviklingen.

Ændringer til kørende systemer skal godkendes af bankens IT-driftsansvarlige i overensstemmelse med gældende regler og procedurer, herunder bankens formelle regler for idriftsætning.

Udvikling af systemer og modeller i værktøjer, som anvendes til ledelsesmæssige beslutninger, skal overholde gældende regler for systemudvikling og drift, herunder gældende design-, løsnings- og referencearkitektur.

4. Risikovurdering og -håndtering (ISO27001:2017, afsnit 6.1.2 og 6.1.3)

Banken anvender en risikovurderingsproces baseret på IT-aktivernes klassifikation, vigtighed, trusler og sårbarheder til at afgøre risikotolerancen, prioriteringen og håndteringen, herunder supplerende sikkerhedsforanstaltninger og imødegående aktiviteter.

IT-anvendelse, IT-systemer, - processer m.m. skal underbygges af en risikovurdering i overensstemmelse med regler og koncept for IT-risikovurderinger, beskrevet i IT-risikostyringspolitikken.

5. Roller, ansvar og beføjelser (ISO27001:2017, afsnit 5.3)

Ansvar
Spar Nords bestyrelse og direktion er overordnet ansvarlige for IT-sikkerheden i banken, jf. de til enhver tid gældende ansvarsbeskrivelser for bestyrelse og direktion i Ledelsesbekendtgørelsens bilag 5.

- **Bestyrelsen**
  Bestyrelsen har ansvaret for at sikre, at virksomheden har en egnet organisering og tilstrækkelig intern styring og kontrol af alle risici i forbindelse med dens IT-anvendelse. Bestyrelsen skal regelmæssigt og mindst én gang om året revurdere og godkende IT-sikkerhedspolitikken på baggrund af en opdateret samlet risikovurdering, der bygger på virksomhedens løbende vedligeholdte IT-risikoregister. Bestyrelsen skal i den forbindelse vurdere, om IT-sikkerhedspolitikken er tilstrækkelig til at sikre, at risici, som IT-anvendelsen medfører og forventes at medføre, er på et acceptabelt niveau for virksomheden.

- **Direktionen**
  Spar Nords direktion er ansvarlig for, at IT-sikkerhedspolitikken, regler og procedurer for IT-sikkerhed og IT-beredskab er etableret og vedligeholdt. Desuden har direktionen ansvar for, at der gennemføres løbende kontroller med IT-sikkerhedspolitikkens efterlevelse, og at der sker rapportering til direktionen og bestyrelse, i overensstemmelse med Ledelsesbekendtgørelsens bilag 5 om IT-sikkerhed.
  Direktionen skal sikre, at der er tilstrækkeligt og kvalificeret personale til løbende at understøtte virksomhedens operationelle IT-behov og IT-risikostyringsprocesser. Direktionen skal sikre, at det tildelte budget er tilstrækkeligt.
  Desuden skal direktionen sikre, at relevante medarbejdere, konsulenter, der beskæftiger sig med området, herunder personer med nøglefunktioner, modtager relevant uddannelse inden for IT-risici, herunder IT-sikkerhed. Direktionen skal sikre, at der udarbejdes og implementeres et uddannelsesprogram, herunder løbende awarenessprogrammer for alle medarbejdere og konsulenter. Det skal sikres, at de uddannes i at varetage deres opgaver og ansvar i overensstemmelse med de relevante IT-sikkerhedspolitikker og -regler, for at reducere menneskelige fejl, tyveri, svig, misbrug eller tab, samt hvordan IT-risici skal styres. Uddannelsesprogrammet skal tilbyde uddannelse mindst én gang om året.
  Spar Nords direktion er desuden ansvarlig for, at der informeres om IT-sikkerhed. Opgaven udføres af den lokale leder i forbindelse med nyansættelser, i forbindelse med ændringer i politik og regler og minimum en gang om året.

- **Direktører og afdelingsdirektører i Spar Nord**
  Alle direktører og afdelingsdirektører i Spar Nord er ansvarlig for den forretningsmæssige IT-sikkerhed samt for formidling af IT-sikkerhed til eget ansvarsområdes medarbejdere, konsulenter og andre relevante samarbejdspartnere.

- **Direktør med procesansvar**
  Den fagansvarlige direktør har ansvaret for, at der findes beskrevne manuelle nødprocedurer og/eller instrukser, dækkende eget fagområde.

- **Direktør for IT**
  Ansvarlig direktør for IT-området, har ansvar for at forvalte direktionens operationelle ansvarsområde vedr. IT-sikkerhed i overensstemmelse med Ledelsesbekendtgørelsens bilag 5. Ansvar omfatter tillige ansvar for at sikre implementering af IT-sikkerhedspolitikken og -regler i Spar Nords IT-infrastruktur samt at gennemføre 1. line compliancekontroller. Ansvarlig direktør for IT har også ansvar for at opdatere og vedligeholde IT-beredskabsplan og IT-reetableringsprocedurer.

- **CISO** (Chief Information Security Officer)
  CISO'en er ansvarlig for at følge op på IT-sikkerhed og IT-risici i medfør af Ledelsesbekendtgørelsens bilag 5, herunder løbende at gennemføre kontrol med overholdelse af IT-sikkerhedspolitikken, -regler og -procedurer for IT-sikkerhed. Desuden er CISO'en ansvarlig for at opdatere og vedligeholde IT-beredskabsmålsætning samt at efterprøve IT-beredskabsplanen minimum en gang årligt.
  CISO'en rapporterer til direktionen og bestyrelsen periodisk, med minimum samme interval, som Risikoansvarliges risikorapportering, samt ved væsentlige afvigelser/hændelser. Ansvaret inkluderer beføjelser til at foretage enhver form for undersøgelse omkring IT-sikkerheden for at kunne udføre sin funktion. Vurderer CISO'en, at der er eller opstår en alvorlig, uafdækket trussel mod IT-sikkerheden, eller at ledelsens målsætninger for IT-sikkerhed ikke overholdes, så har CISO'en ledelsens beføjelser til at foretage nødvendige beslutninger, til at standse truslen og stille krav om forbedrede tiltag til håndtering af risikoen ved truslen. Gør CISO'en brug af denne beføjelse, har CISO'en pligt til straks at rapportere til Direktionen i umiddelbar forlængelse heraf.

- **Systemejer**
  Der skal være udpeget en forretningsmæssig ansvarlig systemejer for alle systemer, der anvendes i Spar Nord og hos leverandører - inklusive cloudløsninger.
  Systemejer har ansvar for
  - at systemet forretningsmæssigt er i overensstemmelse med de nødvendige behov
  - at systemet er compliant (overholder gældende regler) med gældende IT-sikkerhedspolitik og -regler
  - at der udarbejdes risikovurderinger på systemer
  - at systemer klassificeres
  - håndtering af revisionsrapporter

- for governance-aftaler, der vedrører systemet
- for systemets strategiske og økonomiske udvikling
- for brugerprofiler i systemet
- varetagelse af den forretningsmæssige funktionalitet overfor leverandøren i samarbejde med ISA'en og BSA'en.
- udarbejdelse af system-roadmap
- for godkendelse af idriftsættelser af nye systemer eller større ændringer til systemer
- bidrag til indgåelse af SLA med leverandører – sammen med BSA og ISA
- at systemer lever op til krav om fortrolighed, tilgængelighed og integritet

- **IT-sikkerhedsudvalg**
  IT-sikkerhedsudvalget understøtter den operationelle styring af informationssikkerhed samt IT-risikostyring i Spar Nord. Udvalget er ansvarlig for at følge op på og behandle IT-sikkerhedsemner og -risici, som kan medføre en væsentlig konsekvens for Spar Nord. Der skal afholdes møder i udvalget minimum en gang i kvartalet..

- **Medarbejder i Spar Nord**
  Den enkelte medarbejder er ansvarlig for minimum en gang om året at sætte sig ind i og løbende efterleve IT-sikkerhedspolitik og -regler for dennes arbejdsområde.

6. Organisering af IT-sikkerhed (ISO27002:2017, afsnit 6)

Koncern IT-sikkerhed er organisatorisk placeret, som selvstændigt ansvarsområde i 2nd Line under Risikostyring. Den strategiske vigtighed af IT-sikkerheden Spar Nord er understreget ved, at CISO'en også rapporterer direkte til direktionen og bestyrelsen.

Det operationelle IT-sikkerhedsansvar varetages af forretningen og IT i 1st Line.

Interne sikkerhedsfora

Der findes følgende formelle IT-sikkerhedsfora i Spar Nord:

- IT-sikkerhedsudvalg, jf. afsnit 5 ovenfor.

Funktionsadskillelse

Der skal sikres funktionsadskillelse mellem udvikling, drift og forretningens anvendelse af systemer. I Spar Nord er al IT-udvikling, IT-drift og de forretningsfunktioner der anvender systemer funktionsadskilt. Det sikres herigennem, at der ikke er personsammenfald mellem funktioner der udfører IT-udvikling, IT-drift og bankens forretningsførelse, og at adgange tildeles på en sådan måde, at ingen enkelt funktion kan få kontrol over alle faser af IT-anvendelsen.

Kontakt til myndigheder i forbindelse med væsentlige hændelser

I tilfælde af hændelser, der har væsentlige konsekvenser for bankens evne til at levere væsentlige tjenester, skal Spar Nord IT uden unødigt ophold indberette hændelsen til Finanstilsynet, Center for Cybersikkerhed samt orientere Koncern IT-Sikkerhed om indberetningen.

Idriftsætning

Idriftsættelse af IT-systemer skal følge gældende proces for ibrugtagning af IT-systemer, hvoraf det sikres, at bankens acceptkrav for drift- og forvaltningsvilkår er opfyldt, forud for ibrugtagningen.

Nøglepersoner

Nøglepersoner, som er de eneste der kan udføre en bestemt opgave, bør undgås.

7. IT-sikkerhed i forhold til medarbejdere (ISO27002:2017, afsnit 7)

Alle medarbejdere og konsulenter skal mindst én gang årligt deltage i et uddannelsesprogram vedrørende IT-sikkerhed. Det skal sikres, at de uddannes i at varetage deres opgaver og ansvar i overensstemmelse med de relevante sikkerhedspolitikker og forretningsgange, for at reducere menneskelige fejl, tyveri, svig, misbrug eller tab.

Nyansatte informeres om deres ansvar i forhold til IT-sikkerhed ved et introduktionsforløb som iværksættes af HR og chefen for medarbejderens arbejdsområde. Opdateringer eller ændringer i forhold til ansvar omkring IT-sikkerhed kommunikeres til medarbejdere i HR-funktionen og awareness-kampagner.

HR afgør i hvilken udstrækning der skal udføres baggrundscheck af nye og eksisterende medarbejdere omkring kvalifikationer, kompetencer, straffeforhold mv.

HR informerer IT-Brugeradministration om fratrædende og fratrådte medarbejdere for, at brugeradgange kan ophøre. Medarbejderens chef sørger for, at IT-sikkerheden opretholdes ved, at arbejdsfunktioner rettidigt overdrages.

8. Styring af IT-aktiver (ISO27002:2017, afsnit 8)

Identifikation og håndtering af IT-aktiver

Der skal føres en opdateret oversigt over Spar Nords IT-aktiver, herunder IT-systemer, netværksudstyr, databaser o.s.v. Denne skal indeholde konfigurationen af IT-aktiverne og indbyrdes afhængigheder mellem de forskellige IT-aktiver for at kunne gennemføre konfigurations- og ændringsstyringsprocesser.

Oversigten over fysiske og logiske IT-aktiver skal være tilstrækkelig detaljeret til at sikre hurtig identifikation af et IT-aktiv, dets placering, sikkerhedsklassifikation og ejerforhold. Indbyrdes afhængigheder mellem IT-aktiver skal dokumenteres med henblik på at bidrage til styring af IT-sikkerhedshændelser, herunder cyberangreb.

IT-aktivers livscyklus skal overvåges og styres for at sikre, at de løbende opfylder og understøtter forretnings- og risikostyringskrav, ud fra en risikobaseret tilgang. Der skal ske overvågning af, om IT-aktiverne understøttes af interne eller eksterne leverandører og udviklere, og om alle relevante patches og opgraderinger er implementeret i henhold til dokumenterede processer. Ligeledes skal det overvåges, om alle relevante patches og opgraderinger installeres på grundlag af dokumenterede processer. Risici som følge af forældede eller ikke-supporterede IT-aktiver skal vurderes og mitigeres.

Der skal være indført mekanismer til kontrol af software-, firmware- og dataintegritet.

Kritiske IT-aktiver

Kritiske IT-aktiver, herunder IT-systemer, data, tværgående afhængigheder, nøgleressourcer og processer, skal løbende identificeres og risikovurderes. Dataejer og systemejer har det løbende ansvar for dette, for hhv. data og systemer.

Klassifikation af systemer og processer

Spar Nord klassificerer sine IT-systemer, data og processer, med henblik på at sikre en gradueret omgang med og håndtering af IT-systemerne, data og processerne. Systemejer/procesejer har ansvaret for dette for egne IT-systemer/processer. Ingen IT-systemer, data og/eller processer må være uklassificerede i Spar Nord.

Klassifikation af data

Data nedarver klassifikation fra det enkelte IT-system, hvor data befinder sig. I øvrigt henvises til Datagovernancepolitikken.

Behandling af fortrolige data

Inden data lagres på fællesdrev og lignende, skal den datahåndterende sikre sig, at data er korrekt sikret (Fortrolighedskravet). Data som ikke er klassificeret som offentlig, som udskrives på papir, efterbehandles i Office-pakken, databehandles til analyseformål m.v., skal opfylde databehandlingskrav i EU-persondataforordningen samt generel lovgivning på området Udarbejdede politikker for opfyldelse af behandlingssikkerhed, skal ses som en del af IT-sikkerhedspolitikken.

Håndtering og sikring af mobile arbejdspladser

Der skal udvises forsigtighed, når mobilt udstyr (bærbare computere, iPads, mobiltelefoner, USB-sticks o.lign.) anvendes på offentlige steder, møderum og andre ubeskyttede områder. Der skal være etableret beskyttelse af udstyret for at undgå uautoriseret adgang til eller offentliggørelse af information, som er lagret og behandlet på dette udstyr.

Mobilt udstyr skal også være fysisk beskyttet mod tyveri, især hvis udstyret efterlades f.eks. i biler og andre transportmidler, hotelværelser, konferencecentre, mødesteder og lignende.

Udstyr, som indeholder vigtig, følsom eller kritisk forretningsinformation, skal enten være under opsyn eller låses fysisk inde, eller sikres ved anvendelse af speciallås, som skal sikre, at udstyret ikke kan fjernes eller tilgås af uvedkommende.

Ved brug af privatejet mobilt udstyr til at tilgå Spar Nords IT-systemer, skal der sikres adskillelse af privat og arbejdsrelateret brug af udstyret.

Udleverede aktiver

Det er HR's ansvar, at der føres en fortegnelse over udleverede IT-aktiver, på baggrund af registreringer fra IT-afdelingen og medarbejderens chef. Dog er undtaget informationsaktiver som anses for forbrugsvarer eksempelvis papir, notesbøger, usb-sticks o.lign. For disse undtagelser har medarbejderen et selvstændigt ansvar for at håndtere sådanne informationsaktiver forsvarligt i overensstemmelse med udstedte IT-sikkerhedsregler samt eventuelle detaljerede instrukser.

Fysisk sikkerhed

Bygningsservice omkring beskyttelse af IT-sikkerheden gennem fysiske nøgler, adgangskort, videoovervågning, forsyning (el, vand, varme og køling) o.lign, påhviler ansvarlig direktør for fysisk sikkerhed.

9. Adgangsstyring (ISO27002:2017, afsnit 9)

Krav til adgangsstyring
Adgange og begrænsninger i adgange til aktiver, data og IT-systemer skal sikre banken og dets medarbejdere mod utilsigtet og uautoriseret adgang. Fysiske som logiske adgangsforanstaltninger skal være indrettet efter aktivernes klassifikationsniveau og på en sådan måde, at der opnås et effektivt beskyttelsesniveau, der modsvarer aktivets værdi og kritikalitet. Ligeledes skal banken sikre, at den råder over nødvendige autentifikationsløsninger og øvrige tekniske foranstaltninger, der tilsvarende er i overensstemmelse med aktivernes klassifikationsniveau.

Administration

Administration af brugerrettigheder og -adgange skal ske centralt i Spar Nords funktion for IT-Brugeradministration. Denne funktion skal varetages af særligt betroede medarbejdere som har tilstrækkeligt indblik og uddannelse i bankens organisation og anvendte system- og serviceportefølje. Funktionen skal tillige udføre kontrol af lederautorisationer for alle ændringer, og rettigheder og adgange skal gives, slettes, trækkes tilbage eller ændres rettidigt.

Autorisation

Autorisation for tildeling af brugerrettigheder og -adgange til medarbejdere og kontrahenter, skal ske efter et organisatorisk nærhedsprincip, og hvor nærmeste chef eller direktør beslutter og autoriserer relevansen og omfanget af tildelingen - ud fra et minimumskriterie.

Periodisk gennemgang og opfølgning

Funktionen for IT-Brugeradministration skal planlægge, dokumentere og facilitere en risiko- og intervalbaseret gennemgang og opfølgning på konti samt brugerprofiler med tilhørende rettigheder- og adgange i samarbejde med chefer eller direktører og/eller system- eller dataejere for at sikre, at adgange til data og bruger- og systemkonti ikke har uaktuelle og vide rettigheder, og at disse slettes, når behovet ikke længere er til stede.

Krav til rettigheder- og adgange

Tildeling af rettigheder- og adgange skal baseres på et minimumskriterie for, hvad der er strengt nødvendigt, for at udføre funktionens opgaver (princippet om "least privilege"), samt at der ikke kombineres adgangsrettigheder, som kan anvendes til at omgå kontrolforanstaltninger (princippet om "funktionsadskillelse"). Alle ændringer til rettigheder og adgange skal logges og være historisk sporbare for hele dets livscyklus.

Krav til brugerkonti

Alle brugerkonti er strengt personlige og skal være personhenførbare til medarbejdere eller kontrahenter. Alle ændringer og handlinger i relationer til brugerkonti skal logges og være historisk sporbare for hele kontoens livscyklus. Brugen af generiske og delte brugerkonti er således ikke tilladt.

Krav til systemkonti

Applikationers adgang til data og IT-systemer skal begrænses til det minimum, der er nødvendigt for at levere den relevante tjeneste. Alle systemkonti skal være dokumenteret med formål, rettigheds-omfang, og udløb samt relation til ansvarlig systemejer.

Styring af privilegerede adgange

Adgange med stærke rettigheder til IT-aktiver, herunder data, IT-systemer og IT-udstyr, skal være begrænset til et absolut minimum, og skal følge regler for brugeradministration, der sikrer dokumentation, risikovurdering, opfølgning og udløb. Anmodning herom kan alene autoriseres via ansvarlig direktør for IT-området eller IT-driftschefen. Det skal sikres, at privilegeret adgange underlægges løbende teknisk kontrol og overvågning samt stærke kontrolforanstaltninger. Fjernadgange til kritiske IT-systemer må kun tildeles efter "need to know"-princippet, samt ved anvendelse af stærke autentifikationsløsninger.

Adgange til fysiske IT-driftslokationer

Tildeling af fysisk adgangsrettighed til IT-driftslokationer kan kun ske ved godkendelse af ansvarlig direktør for IT-området eller IT-driftschef.

Særlige forhold via fjernadgang

Brugere med adgange til bankens systemer og data på mobilt udstyr, adgange udenfor bankens normale forretningslokaler samt på udstyr, der ikke er ejet af banken, d.v.s. i offentligt rum, har et særligt ansvar, der skal sikre, at bankens tavshedspligt jf. Lov om finansiel virksomhed §117 (Videregivelse af fortrolige oplysninger) og EU-Persondataforordningen, efterleves.

10. Brug af kryptering (ISO27002:2017, afsnit 10)

Der skal benyttes passende kryptering af informationsaktiver for at sikre mod uvedkommende adgang til Spar

Nords data. Beskyttelsesgraden skal være afstemt med aktivets kritikalitet samt, når logisk adgangskontrol ikke er tilstrækkelig.

Informationsaktiver skal krypteres, hvis de opbevares eller behandles under forhold, hvor der er risiko for, at uvedkommende kan få adgang eller kendskab til dem. Se endvidere afsnit 13 nedenfor vedr. transport/kommunikation af informationer.

11. Fysisk sikkerhed (ISO27002:2017, afsnit 11)

Der er en nær sammenhæng mellem den fysiske sikkerhed, IT-sikkerheden og den generelle sikkerhed i organisationen. Der skal derfor stilles nødvendige krav til lokaliteter, der indeholder IT-udstyr eller andre informationsaktiver, for så vidt angår beskaffenhed og indretning, herunder adgangskontrol, rumsikring, brandsikring, strømforsyning, køling etc. svarende til udstyrets klassifikation, karakter og betydning.

Beskyttelse af informationsaktiver mod ydre trusler henhører under chefen for fysiske sikkerhed. Der henvises også til understøttende IT-sikkerhedsregler for den interne fysiske sikkerhed i forhold til gæster, besøgende, rengøring, andre kolleger mv.

Der skal være implementerede og dokumenterede fysiske sikringsforanstaltninger i relation til IT-aktiver, med formål at beskytte ejendomme, datacentre og følsomme områder mod uautoriseret adgang, tyveri, oversvømmelse, vandskade, brand kemikalieudslip og strømsvigt, som kan ødelægge IT-aktiverne.

Fysiske adgange til IT-systemer må kun tillades for autoriserede personer. Tilladelse skal gives i overensstemmelse med den enkeltes opgaver og ansvarsområder samt begrænses til personer, der er tilstrækkeligt uddannet og overvåget. Fysiske adgangsrettigheder skal regelmæssigt gennemgås. Foranstaltninger til beskyttelse mod klima- og miljøfarer skal stå i et rimeligt forhold til bygningernes betydning og kritikaliteten af den drift eller de IT-systemer, der er placeret i bygningerne.

12. Driftssikkerhed (ISO27002:2017, afsnit 12)

Drift

Drift af IT-installationer i Spar Nord og hos leverandører skal ske efter dokumenterede driftsplaner og vejledninger. Driften skal være sikker og stabil, hvilket skal sikres gennem størst mulig automatisering, kontrol og løbende kapacitetstilpasning. Hos leverandører skal dette sikres ved skriftlige aftaler og kontrol.

Potentielle sårbarheder skal identificeres, vurderes og afhjælpes ved opdatering af software og firmware, herunder software, der anvendes af virksomhedens interne og eksterne brugere.

Sikring af IT- og supporterende aktiver (netværk og infrastruktur) skal beskyttes ved brug af konfigurationsstandarder og templates med et niveau af foranstaltninger der er relevant ifht. klassifikationsgraden.
Der skal være implementeret netværkssegmentering, systemer til at forebygge datatab og kryptering af netværkstrafik, så det på tilfredsstillende vis modsvarer bankens trusselsbillede.

De enheder, som brugere har adgang til, herunder systemer, servere, arbejdsstationer og mobile enheder, skal beskyttes. Ligeledes skal det vurderes, om enhederne opfylder de sikkerhedsstandarder, der er fastlagt, før enhederne tilsluttes virksomhedens netværk.

Data skal ved opbevaring og overførsel være krypterede ud fra en klassificering og risikovurdering.

Der skal løbende vurderes, om ændringer i produktionsmiljøer påvirker sikkerhedsforanstaltningerne eller kræver, at yderligere foranstaltninger implementeres for at mitigere de hermed forbundne risici tilstrækkeligt. Disse ændringer skal indgå i Spar Nords formelle ændringsstyringsproces, som skal sikre, at ændringer risikovurderes, planlægges, testes, dokumenteres, godkendes og installeres korrekt.

Backup

Spar Nord skal have et effektivt reetableringsmiljø til genetablering (restore) af data og IT-systemer.

Der skal foretages sikkerhedskopiering af programmer, systemindstillinger og data, der sikrer mulighed for reetablering af normal drift indenfor de fastlagte tidsrammer samt sikrer, at data kan reetableres indenfor den lovbestemte arkiveringsfrist. Der skal ligeledes være beskrevet regler som fastsætter backup frekvens, som

minimum overholder gældende lovgivning for opbevaring og frekvens af backup.

Backup skal være adskilt i to datacentre, placeret på hver sin geografisk adskilte lokation. Backup skal være hinanden redundante. Backup-systemet skal designes sådan, at alle backup som udgangspunkt gemmes på begge datacentre, således at der altid er fuld back-up på begge datacentre.
Forretningskritiske data (exportdata), der skal gemmes i længere tid til en fysisk serverløsning, skal være placeret på en tredje lokation forskellig fra de to datacentre.

Der skal altid forefindes udstyr og foranstaltninger, der sikrer at systemer og data kan reetableres.

Samme person må ikke ukontrolleret have adgang til både originaldata og kopidata.

Logning og overvågning

Spar Nord logger og overvåger bankens IT-anvendelse, herunder netværk, IT-udstyr og IT-services. Formålet er at kunne identificere enhver adgang og anvendelse, som strider imod eller kræves logget efter love, politikker og regler. Yderligere anvendes log og overvågning til at opdage hændelser tidligt, så Spar Nord kan inddæmme og reducere eller eliminere hændelser.

Systemejer og IT har ansvar for at vurdere behovet for hændelseslogning samt behov for opbevaring, gennemgang og overvågning heraf. Dette afdækkes ved en risikovurdering af det enkelte system.

Alle relevante aktiviteter, og som minimum de aktiviteter der udføres af privilegerede brugere, skal logges og overvåges. Adgangslogs skal sikres, så uautoriseret ændring eller sletning forhindres, og skal opbevares i en periode for de identificerede forretningsfunktioner, understøttende processer og IT-aktiver. Oplysningerne skal bruges, som led i identifikationen og undersøgelse af uregelmæssige aktiviteter.

Anskaffelse/reparation/bortskaffelse af IT-udstyr og infrastruktur

Anskaffelse og vedligehold af IT-udstyr og infrastruktur skal ske i IT eller i et samarbejde med ansvarlig direktør for IT-området.
Anskaffelse, vedligeholdelse og bortskaffelse af it- og supporterende aktiver må alene ske via bankens it-driftsafdeling, der tilsikrer, at udvælgelse og valg af teknologi er i overensstemmelse med valgte arkitektur, samt at korrekte leverandører anvendes til vedligeholdelse og bortskaffelse af aktiverne, inkl. datasletning og dokumentation herfor.

IT-udstyr og medier skal bortskaffes på forsvarlig og sikker vis, når der ikke længere er brug for udstyret. I tilfælde af videresalg, skal alt data slettes effektivt fra udstyret.

13. Kommunikationssikkerhed (ISO27002:2017, afsnit 13)

Kommunikation skal ske ved passende sikkerhedsforanstaltninger, som for elektronisk kommunikation til eksterne stiller krav om kryptering i overensstemmelse med underliggende regler for kryptering.

Øvrig kommunikation skal iagttage fornøden agtpågivenhed, således at fortrolighedskrav mv. overholdes, såvel i forhold til skriftlig som verbal kommunikation.

Ved aftale om informationsoverførsler, herunder også informationsoverførsler til 3. mand, skal sikkerheden være dokumenteret. Information i netværk og understøttende informationsbehandlings-faciliteter skal sikres via nødvendig netværksstyring, sikring af netværkstjenester og opdeling af netværk.

Ved informationsoverførsel til 3. part, skal politik for håndtering af leverandører (Politik for outsourcing af aktivitetsområder i Spar Nord) følges, for at sikre, at nødvendige aftaler herom er dokumenteret, at informationen er beskyttet med relevante foranstaltninger svarende til klassifikationsniveauet.

14. IT-sikkerhed for anskaffelse, udvikling og vedligeholdelse af systemer (ISO27002:2017, afsnit 14)

Udvikling og vedligeholdelse af IT-systemer

Udvikling og vedligeholdelse af systemer skal ske efter en aftalt systemarkitektur- og udviklingsmetode. Metoden skal blandt andet sikre, at der sker tilstrækkelig kvalitetssikring af udviklede systemer/modeller, herunder f.eks. kravspecifikation, dokumentation og systemgodkendelsestest.

Ved udvikling af systemer og modeller, der anvendes til forretningsmæssig beslutningstagning, såvel internt som eksternt, skal der udarbejdes/forefindes dokumentation af systemet/modellen.

De udviklede systemer/modeller skal indeholde automatiske eller manuelle kontroller.

Der må kun forefindes og anvendes godkendt og licenseret programmel på bankens IT-udstyr. Udlån af bankens software/programmer er ikke tilladt ligesom software ikke må fjernes fra bankens lokaliteter.

Systemændringer i banken skal følge de gældende regler for idriftsætning og/eller Change Management procedurer, ligesom ændringer skal være dokumenterede og gennemførelse godkendt ved underskrift. Tillige skal dette være dokumenteret i aftaleforholdet med eksterne leverandører.

Funktionelle og ikke-funktionelle krav, herunder krav til informationssikkerhed, defineres klart og godkendes af den relevante leder, inden IT-systemer anskaffes eller udvikles.

IT-systemer skal testes og godkendes, inden de tages i brug, og der skal tages højde for forretnings-processernes og aktivernes kritikalitet. Testmiljøer skal i tilstrækkelig grad afspejle produktionsmiljøet.

Der skal endvidere etableres adskilte miljøer for at sikre funktionsadskillelse, og hindre ikke-verificerede ændringer til produktionssystemerne. Produktionsmiljøerne skal på baggrund af en risikovurdering, adskilles fra øvrige miljøer og integrationer.

Samtidig skal integriteten og fortroligheden af produktionsdata, der anvendes i ikke-produktions-miljøer, sikres og om nødvendigt pseudonymiseres/anonymiseres. Adgang til produktionsdata skal være strengt begrænset for autoriseret adgang.

Der skal implementeres foranstaltninger til at beskytte integriteten af kildekoden til IT-systemer. Udviklingen, implementeringen, driften og/eller konfigurationen af IT-systemerne skal dokumen-teres, for at minimere unødvendig afhængighed af individer og ekspertviden.

Dokumentationen for IT-fagsystemer som drives af banken og underleverandører, skal som minimum omfatte brugerdokumentation, teknisk systemdokumentation og tilhørende forretnings-gange for systemforvaltningen.

Kravene for anskaffelse og udvikling af IT-systemer skal også gælde for IT-systemer, der udvikles eller håndteres af forretningsfunktionernes brugere uden for IT-organisationen. Dette skal ske ud fra en risikobaseret tilgang.

Anskaffelse af IT-systemer

Anskaffelse af systemer skal altid ske i overensstemmelse med IT-politikken.

Enhver anskaffelse af IT-systemer skal ske på baggrund af en risikovurdering efter gældende model for risikostyring samt IT-risikostyringspolitik.

15. IT-sikkerhed i forhold til leverandører (ISO27002:2017, afsnit 15)

IT-sikkerhed i leverandørforhold

Aftaler der indgås med eksterne leverandører skal overholde Spar Nords til enhver tid gældende politik for outsourcing, herunder indeholde oplysninger om, at Spar Nords eksterne revisor eller Spar Nord kan indhente fornødne oplysninger om forhold vedrørende IT-sikkerheden hos leverandøren og/eller at det er aftalt med den eksterne leverandør, at der modtages revisionserklæring fra leverandørens revisor om IT-sikkerheden.

Systemejeren har ansvaret for at informere IT-Drift om kontraktlige krav fra leverandører om involvering, informering eller lignende ved sikkerhedsbrud, således at disse krav korrekt understøttes i styringen af IT-sikkerhedsbrud.

Mitigerende foranstaltninger, når IT-tjenesters, betalingstjenesters og IT-systemers operationelle funktioner outsources, herunder til koncernenheder, skal være effektive. De mitigerende foranstaltninger skal være defineret i henhold til IT-risikostyringen.

Det skal ved aftale sikres, at der skal foreligge den samme sikkerhed, i forbindelse med opbevaring af Spar Nords data, som var data opbevaret i Spar Nord.

For at opretholde sikkerhedsniveauet og sikre kontinuitet i IT-tjenesterne og IT-systemerne, skal kontrakter og serviceleveranceaftaler indgået med leverandører indeholde et sæt af sikkerhedskrav som angivet i politik for håndtering af leverandører:

- Passende og forholdsmæssige IT-sikkerhedsmål og foranstaltninger
- Forretningsgange for styring af IT-sikkerhedshændelser, herunder eskalering og rapportering

Leverandørers grad af efterlevelse af IT-sikkerhedsmål, sikkerhedsforanstaltninger og servicemål skal overvåges og rapporteres i relevant omfang.

Leverandøruafhængighed

Spar Nord vil sikre leverandøruafhængighed, hvor det er praktisk muligt. Der skal være aftaler med leverandører, der sikrer daglig drift, Task Force og katastrofesituationer.

16. Styring af IT-sikkerhedsbrud (ISO27002:2017, afsnit 16)

Et væsentligt element i IT-sikkerheden er, at Spar Nord er i stand til at opdage og reagere rettidigt på IT-sikkerhedsbrud, for at standse eller begrænse konsekvenserne. Alle medarbejdere og samarbejdspartnere af enhver art, er forpligtigede til at indrapportere enhver IT-sikkerhedshændelse til IT, og Juridisk Afdeling/DPO ved mistanke om persondatabrud. IT-Drift har kontakt til relevante myndigheder og forestår indrapportering hertil.

IT-hændelses- og problemstyring skal overvåge og logge IT-sikkerhedshændelser og gøre det muligt for Spar Nord at fortsætte eller genoptage kritiske forretningsfunktioner og -processer rettidigt, når der opstår driftsforstyrrelser. IT-sikkerhedshændelser skal klassificeres ud fra passende kriterier og tærskler samt fastsætte tidlige varslingsindikatorer, der skal fungere som alarmer for at muliggøre tidlig opdagelse af IT-sikkerhedshændelser.

Med henblik på at minimere påvirkningen af utilsigtede IT-sikkerhedsbrud og -hændelser og muliggøre rettidig genopretning, skal der være etableret og dokumenteret en konsekvent og integreret overvågning, styring og opfølgning på IT-sikkerhedshændelser. Desuden skal de grundlæggende årsager identificeres, undersøges og fjernes for at forhindre, at IT-sikkerhedshændelser gentages. Dokumentation skal indeholde krav til identifikation, sporing, registrering, kategorisering, klassificering og rapportering af IT-sikkerhedshændelser prioriteret på baggrund af forretningskritikaliteten. Roller og ansvar for forskellige hændelsesscenarier skal beskrives. Det samme er gældende for IT-problemstyring, med henblik på at identificere, analysere og løse årsagen bag IT-sikkerhedshændelser. IT-sikkerhedshændelser, der kan påvirke

virksomheden, som er blevet identificeret eller har fundet sted inden for og/eller uden for organisationen, skal analyseres. Ligeledes skal de vigtigste erfaringer tages i betragtning, og sikkerhedsforanstaltningerne skal opdateres i overensstemmelse hermed.

Det er IT's ansvar at etablere effektive interne kommunikationsplaner, herunder notificering om IT-sikkerhedshændelser og eskalationsprocedurer, der også omfatter sikkerhedsrelaterede kundeklager, for at sikre, at IT-sikkerhedshændelser med potentielt stor negativ indvirkning på kritiske IT-systemer og IT-tjenester rapporteres til den relevante ledelse, at direktionen underrettes i tilfælde af væsentlige IT-sikkerhedshændelser og som minimum underrettes om konsekvenserne, opfølgningen og de yderligere kontrolforanstaltninger, der skal udarbejdes og implementeres som resultat af it-sikkerhedshændelserne, og at bestyrelsen underrettes i relevant omfang.

Der skal ske mitigering af konsekvenserne, som følge af IT-sikkerhedshændelserne, og det skal sikres, at tjenesten rettidigt bliver operationel og sikker.

Der skal være etableret specifikke eksterne kommunikationsplaner for kritiske forretningsfunktioner og processer for at sikresamarbejde med relevante interessenter, for effektivt at kunne reagere på hændelsen og reetablere driften, og levering af rettidige oplysninger til eksterne parter, og i overensstemmelse med gældende lovgivning.

IT-sikkerhedshændelser, der medfører væsentlig reduktion i funktionaliteten, som følge af brud på fortrolighed, integritet og/eller tilgængelighed til IT-systemer og/eller data, uden unødigt ophold bliver rapporteret til Finanstilsynet. Rapporteringen skal omfatte IT-sikkerhedshændelser, som virksomheden selv kategoriserer som alvorlige og/eller kritiske, men skal også omfatte andre afvigelser, hvis disse afdækker specielle sårbarheder i en applikation, arkitektur, infrastruktur, m.v.

Der skal foretages forretningskonsekvensanalyser (Business Impact Analysis, BIA). Dette skal gøres ved at analysere eksponeringen over for væsentlige driftsforstyrrelser og vurdere potentielle konsekvenser kvantitativt og kvalitativt ved hjælp af interne og/eller eksterne data og scenarieanalyser. Der skal tages højde for fortrolighed, integritet og tilgængelighed. Forretningskonsekvensanalyserne skal også inddrage kritikaliteten af de identificerede og klassificerede forretningsfunktioner, understøttende processer, tredjeparter og IT-aktiver, deres indbyrdes afhængigheder, samt behov for redundans.

Det skal sikres, at IT-systemer og IT-tjenester er designet og tilpasset virksomhedens forretningskonsekvensanalyser, f.eks. ved at sikre redundans af kritiske komponenter for at undgå driftsforstyrrelser forårsaget af hændelser, der påvirker disse komponenter.

17. IT-sikkerhedskrav til IT-beredskab (ISO27002:2017, afsnit 17)

Beredskabs- og genopretningsplaner

På grundlag af forretningskonsekvensanalyserne (BIA), og mulige scenarier, skal der udarbejdes og implementeres beredskabs- og genopretningsplaner (DRP) og forretningskontinuitetsplaner (DRP). Disse planer skal beskrive, hvilke betingelser, der kan medføre aktivering af planerne, og hvilke foranstaltninger der skal træffes for at sikre tilgængelighed, kontinuitet og genopretning af, virksomhedens kritiske IT-systemer og IT-tjenester. Beredskabs- og genopretningsplanerne skal sikre, at genopretningsmålene kan opnås, i overensstemmelse med Målsætning for beredskabet.

Beredskabs- og genopretningsplanerne skal tage højde for både kort- og langsigtede genopretningsmuligheder. Planerne skal fokusere på at genoprette driften af kritiske forretningsfunktioner, understøttende processer, IT-aktiver og deres indbyrdes afhængigheder for at undgå negative påvirkninger på virksomheders drift og på det finansielle system, herunder på betalingssystemer og på betalingstjenestebrugere og for at sikre gennemførelse af udestående betalingstransaktioner.

Beredskabs- og genopretningsplaner skal dokumenteres og stilles til rådighed for relevante interessenter samt være let tilgængelige i nødsituationer.

De skal opdateres i overensstemmelse med erfaringerne fra IT-sikkerhedshændelser, test, nye identificerede risici og trusler samt ved ændrede genopretningsmål og -prioriteter.

I planerne skal der også tages stilling til alternative muligheder i tilfælde af, at det på kort sigt ikke er muligt at genoprette IT-driften på grund af omkostninger, risici, logistik eller uforudsete omstændigheder.

Som led i beredskabs- og genopretningsplanerne skal der tages stilling til og implementeres nødplansforanstaltninger for at mitigere svigt fra leverandører, som er af afgørende betydning for den fortsatte drift af Spar Nords IT-tjenester.

Test af planer

Planerne skal testes regelmæssigt. Planerne for kritiske funktioner, understøttende processer, IT- aktiver og disses indbyrdes afhængigheder skal testes mindst én gang om året, herunder, hvis relevant, dem der leveres af tredjeparter.

Planerne skal opdateres mindst én gang om året og på grundlag af testresultaterne, det aktuelle trusselsbillede og erfaringerne fra tidligere IT-sikkerhedshændelser. Ændringer i genopretningsmålene (herunder RTO'er og RPO'er) og/eller ændringer i forretningsfunktioner, understøttende processer og IT-aktiver skal også, hvor det er relevant, medføre opdatering af planerne.

Test af planerne skal vise, at det er muligt at opretholde virksomhedens forretningsaktiviteter, indtil kritiske funktioner bliver genoprettet. Planerne skal som minimum omfatte test af flere alvorlige men plausible scenarier, inklusiv dem der tages i betragtning i forbindelse med udviklingen af planerne. Dette gælder også for test af tjenester udbudt af tredjeparter. Test skal også omfatte skift af kritiske forretningsfunktioner, understøttende processer og IT-aktiver til virksomhedens katastrofeberedskab for at vise, at de kan fungere under disse omstændigheder i en repræsentativ periode, og at Spar Nord kan tilbageføre aktiviteterne til normal drift.

Test skal være designet til at udfordre de antagelser, som planerne er baseret på, herunder governance og krisekommunikationsplaner. Den skal omfatte krav til at efterprøve medarbejdernes, konsulenternes, IT-systemernes og IT-tjenesternes evne til at reagere hensigtsmæssigt på de identificerede scenarier.

Testresultaterne skal dokumenteres, og at eventuelle identificerede afvigelser analyseres, adresseres og rapporteres til en relevant leder, samt direktion og bestyrelse når dette er relevant.

Krisekommunikation

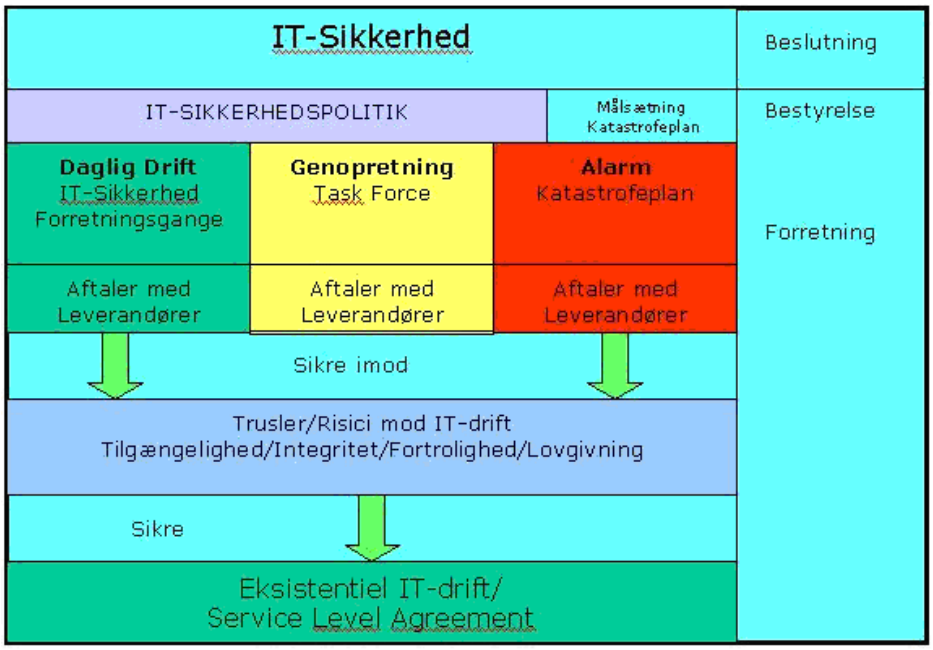
I tilfælde af nedbrud eller nødsituationer og under gennemførelsen af forretningskontinuitetsplanerne skal Spar Nord have effektive krisekommunikationsforanstaltninger, så alle relevante interne og eksterne interessenter underrettes rettidigt og på en hensigtsmæssig måde. Dette omfatter bl.a. de kompetente myndigheder og eksterne tjenesteudbydere, leverandører og/eller koncernenheder.

På den efterfølgende tegning er de væsentlige elementer indplaceret i sammenhæng.

GRØN viser, at sikkerhed hovedsageligt er en del af dagligdagen, som reguleres af regler for IT-sikkerhed.

GUL viser, at IT-ledelsen og den forretningsmæssige systemejer vurderer, at der kan etableres en normal situation, inden grænsen for katastrofe træder i kraft.

RØD viser, at her iværksætter IT-ledelsen og den forretningsmæssige systemejer den etablerede beredskabsplan. En katastrofe kan være tab af data, tab af system, tab af maskinkraft, tab af datalinjer eller mere fysisk orienterede hændelser, som vandskade, flystyrt eller terror.



Flercenterdrift

For alle forretningskritiske systemer, skal der tages stilling til, hvorvidt der er behov for etablering af flercenterdrift for det givne system. Denne stillingtagen skal være baseret på en konkret risikovurdering for det enkelte system, og skal revurderes årligt. Ansvar for udarbejdelse af risikovurdering beror hos den pågældende systemejer, herunder risikovurderingens indhold og konklusion.

Spar Nord vil have en primær og en sekundær driftslokation for egne driftede IT-systemer og IT-infrastruktur. Disse skal være placeret på to geografisk adskilte lokationer med passende afstand, for at sikre en effektiv afvikling af den daglige drift samt en hurtig genopretning af driften af bankens vitale systemer i en katastrofesituation.

Direktionen er ansvarlig for at risikovurdere, hvorvidt afstanden mellem de forskellige driftscentre er passende.

For eksterne løsninger (Eksemplevis Cloud-løsninger og outsourcing), skal der være en risikovurdering i forbindelse med anskaffelsen, om der stilles krav om adskilte driftslokationer.

18. Compliance (ISO27002:2017, afsnit 18)

Der gælder omfattende lov om finansiel virksomhed med tilhørende lovkrav, øvrig lovgivning, eksempelvis EU-Persondataforordningen, sektorkrav i øvrigt samt krav fra interessenter og ledelsen.

Compliance sker hermed gennem et effektivt og kontinuerligt arbejde i ledelsesstyringen af IT-sikkerheden.

Løbende fokus, arbejde i hverdagen og regelmæssige møder udføres for at opnå compliance, hvilket sammen med kontinuerlige forbedringer, resultater af tilsynsgennemgang (Inspektioner fra Finanstilsyn, intern/ekstern revision, compliance) og ledelsesgennemgange skal tilsikre, at mangler identificeres og afhjælpes.

19. Afvigelser (ISO27001:2017, afsnit 9)

Alle afvigelser fra IT-sikkerhedspolitikken er tidsbegrænsede og skal godkendes skriftligt af bankens Direktion via

gældende proces for behandling af dispensationer. Det er IT-sikkerhedsudvalgets opgave at kvalificere dispensationsønsker fra IT-sikkerhedspolitikken, forud for endelig direktionsgodkendelse.

Alle afvigelser fra IT-sikkerhedsreglerne er tidsbegrænsede og skal godkendes skriftligt af IT-sikkerhedsudvalget via gældende proces for behandling af dispensationer.

Afvigelser fra de gældende IT-sikkerhedspolitik og -regler må udelukkende finde sted på baggrund af en risikovurdering. Ansvarlig forretningsdirektør, dataejer og/eller systemejer er ansvarlig for udarbejdelse af risikovurdering, herunder risikovurderingens indhold og konklusion.

Ved introduktion af en afvigelse, gives tidsbegrænset dispensation, så det kan sikres, at mitigerende tiltag kan implementeres i overensstemmelse med afvigelsens risiko og kritikalitet og uden unødig forsinkelse.

Så længe dispensationen er gældende, skal der etableres alternative sikkerhedsforanstaltninger, så det til enhver tid gældende sikkerhedsniveau kan overholdes.

IT-sikkerhedsudvalget skal minimum to gange årligt rapportere på bevilgede dispensationer til Direktionen.

20. Opfølgning (ISO27001:2017, afsnit 9)

Spar Nord Bank måler, vurderer og følger op på IT-sikkerheden, ad hoc eller på baggrund af årshjul, på følgende måde:

- Entydig registrering og opfølgning på hændelser indenfor IT-sikkerhedsområdet
- Registrering af alle tiltag indenfor IT-sikkerhedsområdet
- Opfølgning på vidensniveau indenfor IT-sikkerhedsområdet i Spar Nord Bank
- Gennemførelse af uafhængige tredjepartskontroller og evalueringer af IT-sikkerheden
- Gennemførelse af kontroller og rapportering på hændelser
- Opfølgning på interne såvel som eksterne kontrollanters besøg i banken, herunder Intern/Ekstern Revision og Finanstilsynet

Test af IT-sikkerheden

Der skal udføres tests, gennemgange og vurderinger af informationssikkerheden for at sikre effektiv identifikation af sårbarheder i IT-systemer og IT-tjenester. Der skal foretages gap-analyser i forhold til informationssikkerhedsstandarder samt gennemgange af overholdelse af regler.

Desuden skal Spar Nord ud fra en risikobaseret tilgang og best practices udføre kildekode-review, sårbarhedsvurderinger, penetrationstest, "Red Team" lignende øvelser m.m.

Det er et krav til test af informationssikkerheden, at effektiviteten af informationssikkerhedsforanstaltningerne valideres. Tests skal tage højde for trusler og sårbarheder, som er identificeret gennem trusselsovervågning og risikovurderingsprocessen.

Der skal ligeledes gennemføres test af sikkerhedsforanstaltninger i tilfælde af ændringer i infrastruktur, processer eller forretningsgange, og hvis der foretages ændringer på grund af større IT-sikkerhedshændelser. Der skal også gennemføres risikobaseret test af egenudviklede lanceringer, som følge af nye eller væsentligt ændrede kritiske applikationer, der kan tilgås fra internettet. Herunder gælder tillige test af egenudviklede betalingstjenester, som Spar Nord måtte udbyde.

Tests af informationssikkerheden skal udføres af uafhængige personer med tilstrækkelig viden, faglig kompetence og ekspertise i test af informationssikkerhedsforanstaltninger, og som ikke er involveret i udviklingen af Spar Nords informationssikkerhedsforanstaltninger.
Tests omfatter sårbarhedsscanninger og penetrationstest, som står i forhold til det risikoniveau, der er identificeret i forretningsprocesser og -systemer.

Kritiske IT-systemer skal testes mindst én gang om året. Ikke-kritiske systemer skal testes regelmæssigt og inden

for en periode på minimum tre år.

Resultaterne af de udførte sikkerhedstest bliver evalueret, med henblik på, at sikringsforanstaltninger opdateres i overensstemmelse hermed uden unødig forsinkelse, når der er tale om kritiske systemer.

Håndtering af IT-revisionsanbefalinger

Der skal ske opfølgning på IT-revisionsanbefalinger med tilhørende risikovurderinger. Endvidere skal der sikres mitigering og efterlevelse af IT-revisionsanbefalinger samt de risici, som anbefalingerne medfører.

21. Sanktionsmuligheder (ISO27001:2017, afsnit 9)

Enhver korrespondance til og fra bankens IT-arbejdspladser kan tænkes uddraget og fremlagt i forbindelse med retshandlinger, der involverer Spar Nord.

Strafbar anvendelse af systemer, data, mail-tjenester, internettjenester m.m. vil blive politianmeldt. Konsekvensen af strafbar anvendelse samt anden form for misbrug, besluttes af bankens direktion.

22. Opdateringer (ISO27001:2017, afsnit 9 og 10)

IT-sikkerhedspolitikken revurderes en gang årligt. Opdateringer skal godkendes af bestyrelsen.

23. Ledelsesgodkendelse (ISO27001:2017, afsnit 9.3)

Denne IT-sikkerhedspolitik er godkendt af Spar Nord Banks Bestyrelse 2022.

24. Revisionshistorik (ISO27001:2017, afsnit 7.5.3.e)

Dato:	Version:	Initialer:	Kommentar:
27.06.2014	2.4	Per Lund-Hansen	Godkendt af Bestyrelsen
17.06.2015	2.5	Per Lund-Hansen	Godkendt af Bestyrelsen
31.08.2016	2.6	Per Lund-Hansen	Godkendt af Bestyrelsen
01.07.2017	2.7	Per Lund-Hansen	Godkendt af Bestyrelsen
01.07.2018	3.0	Per Lund-Hansen	Godkendt af Bestyrelsen
19.06.2019	3.1	Per Lund-Hansen	Godkendt af Bestyrelsen
17.06.2020	3.2	Per Lund-Hansen	Godkendt af Bestyrelsen
22.06.2021	3.3	Anders Lehmann Pultz Knudsen	Godkendt af Bestyrelsen
01.07.2022	3.4	Anders Lehmann Pultz Knudsen	Godkendt af Bestyrelsen