Spar Nord

Informationssikkerhedspolitik

1. Målsætning og dækning

Denne Informationssikkerhedspolitik har til formål at sikre et passende sikkerhedsniveau for Bankens IT-aktiver, i forhold til alle interne eller eksterne og utilsigtede eller bevidste trusler. Det skal sikres, at integriteten, fortroligheden og tilgængeligheden af informationer overholdes og tillige er i overensstemmelse med Bankens dataetik.

Politikken fastlægger tillige Bankens sikkerhedsniveau, på baggrund af bestyrelsens overordnede stillingtagen til Bankens risikoprofil, herunder afledte behov og krav til nødvendige sikkerhedsforanstaltninger og kontroller, igennem de beskrevne sikkerhedsprincipper.

Banken er af Finanstilsynet udpeget som Systemisk Vigtigt Finansielt Institut (SIFI) og driver dermed tjenester, som er væsentlige for det samlede finansielle system i Danmark. Bankens finansielle tjenester er digitaliserede og baseres i høj grad på anvendelsen af IT, hvorfor Banken skal sikre et højt niveau for Informationssikkerhed.

Målsætning

Politikkens overordnet mål er at sikre kontinuitet i kritiske forretningsaktiviteter, ved at sikre, at:

- alle informationer, der behandles, opbevares, handles eller frigives af Banken, er af absolut integritet
- alle informationer er tilgængelige og vil blive overvåget og opbevaret i overensstemmelse med procedurerne for opretholdelse af fortrolighed
- sørge for valg af passende sikkerhedsforanstaltninger, for at beskytte IT-aktiverne, give tillid til Bankens interessenter og sikre en effektiv IT-sikkerhedsstyring
- Banken overholder og opfylder gældende lovgivning og sektorkrav samt sin rolle i den samlede danske, finansielle IT-infrastruktur, som SIFI-institut

Dækning

Denne politik er gældende for Bankens organisation, underliggende entiteter, dets medarbejdere og samarbejdspartnere og kontrahenter.

2. Sammenhæng mellem IT-risikoprofil og Bankens sikkerhedsniveau

Bankens direktion er ansvarlig for, at der årligt gennemføres en overordnet risikovurdering af Bankens trusler og sårbarheder, som danner grundlag for Bankens IT-risikoprofil, og som skal godkendes af bestyrelsen. Risikoprofilen er styrende for denne Informationssikkerhedspolitik, der via sikkerhedsprincipperne, understøttende sikkerhedsforanstaltninger og kontroller, skal sikre det nødvendige, og af bestyrelsen ønskede, sikkerhedsniveau.

Forhold vedr. BEC

Bestyrelsen har besluttet at outsource væsentlige og kritiske dele af IT-drift og -udvikling af IT-løsninger til BEC. Det er et krav, at der implementeres specifikke foranstaltninger til at sikre, at sikkerhedsniveauet og efterlevelsen af den besluttede risikoappetit opretholdes i relation til de outsourcede ydelser.
Banken er medejer af samt tilsluttet BEC, der som fælles datacentral bl.a. er underlagt Bekendtgørelse om ledelse og styring af pengeinstitutter m.fl. og bekendtgørelse om systemrevisionens gennemførelse i fælles datacentraler.

Forhold vedr. øvrige væsentlige leverandører

For øvrige væsentlige leverandører, der er udpeget, som kritiske eller vigtige, jf. kriterierne i Politik for outsourcing af aktivitetsområder, skal der sikres tilsvarende foranstaltninger til opretholdelse og overvågning af sikkerhedsniveauet.

IT-sikkerhedsniveau

Sikkerhedsniveauet skal sikre, at de risici, som anvendelsen af IT medfører, er afstemt med Bankens risikoprofil, som er accepteret af bestyrelsen. Niveauet skal modsvare udviklingen i trusselsniveauet, baseret på risikovurderinger samt sikre efterlevelse af gældende regulering indenfor finanssektoren.

Niveauet skal medvirke til, at Banken og dens leverandører er i stand til at oppebære et forsvar imod cybertrusler, bestående af tilstrækkelige teknologiske foranstaltninger, procedurer og medarbejderressourcer. Det kræves, at leverandører af IT-systemer og anvendelsen heraf, skal have en robusthed, som kan sikre stabil drift af Bankens forretningsprocedurer samt sikre et forsvar, som er effektiv over for cyberangreb fra aktuelle trusselsaktører.

Derudover suppleres Informationssikkerhedspolitikken af politikerne for outsourcing, IT-risikostyring og målsætning for IT-beredskab samt ISO/IEC 27001 rammeværket med tilhørende sikkerhedsforanstaltninger, regler og procedurer, som beskriver hvorledes kravene heri operationaliseres.

3. Organisation og ansvar

Bankens bestyrelse og direktion er overordnet ansvarlige for Informationssikkerheden i banken, jf. de til enhver tid gældende ansvarsbeskrivelser for bestyrelse og direktion i Ledelsesbekendtgørelsens bilag 5.

Bankens direktion er ansvarlig for udarbejdelse, ajourføring og efterlevelse af Informationssikkerhedspolitikken, og Bankens 2. forsvarslinje IT-sikkerhedsfunktion varetager den daglige forvaltningsopgave på vegne heraf. Den skal godkendes af Bankens bestyrelse og offentliggøres og kommunikeres til medarbejdere og relevante eksterne parter. Ajourføring skal som minimum foretages hvert år eller ved større ændringer i Bankens risikobillede og/eller aktivsammenhænge.

Roller, ansvar og beføjelser

Bestyrelsen
Bestyrelsen har ansvaret for at sikre, at Banken 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 Informationssikkerhedspolitikken på baggrund af en opdateret, overordnet risikovurdering, der bygger på Bankens løbende, vedligeholdt IT-risikoregister og aktuelle trussels- og sårbarhedsbillede.

Bestyrelsen skal i den forbindelse vurdere, om Informationssikkerhedspolitikken er tilstrækkelig til at sikre, at risici, som IT-anvendelsen medfører og forventes at medføre, er på et acceptabelt niveau for Banken, at direktionen støtter op om Informationssikkerhedspolitikken, ved at udstikke klare informationssikkerhedskrav, udvise synligt engagement og sikre en præcis placering af ansvar.

Bestyrelsen har endvidere ansvar for, mindst en gang årligt, at fastsætte en overordnet målsætning for Bankens IT-beredskab.

Direktionen
Bankens direktion er ansvarlig for, at bestyrelsens målsætning for informationssikkerhed implementeres og efterleves i Banken, samt at Informationssikkerhedspolitikken, understøttende krav og procedurer for informationssikkerhed og IT-beredskab er etableret, vedligeholdt og tager højde for gældende lovgivning for Banken.

Bankens direktion skal sikre, at roller og ansvar for informationssikkerhed er dokumenteret og implementeret i Banken, at der foretages en løbende trusselsvurdering, og at der findes en procedure for håndtering af afvigelser og undtagelser, herunder brud, på informationssikkerheden.

Desuden har direktionen ansvar for, at der gennemføres løbende kontroller med Informationssikkerhedspolitikkens efterlevelse, og at der sker rapportering til direktionen og bestyrelsen, i overensstemmelse med Ledelsesbekendtgørelsens bilag 5's, om informationssikkerhed.

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 og informationssikkerhed. Direktionen skal sikre, at der udarbejdes og implementeres et uddannelsesprogram, herunder løbende awareness-programmer, for alle medarbejdere og konsulenter. Det skal sikres, at de uddannes i at varetage deres opgaver og ansvar i overensstemmelse med de relevante informationssikkerhedspolitikker og -krav, med det formål at reducere risikoen for menneskelige fejl, tyveri, svig, misbrug eller tab, samt i, hvordan IT-risici skal styres. Uddannelsesprogrammet skal tilbyde uddannelse for Bankens medarbejdere og konsulenter mindst én gang om året.

Bankens direktion er desuden ansvarlig for, at der generelt informeres om informationssikkerhed. Opgaven udføres af den personaleansvarlige leder i forbindelse med nyansættelser, og i forbindelse med ændringer til Informationssikkerhedspolitikken og de understøttende informationssikkerhedskrav, og minimum en gang om året.

Direktører og afdelingsdirektører i Banken
Alle direktører og afdelingsdirektører i Banken er ansvarlige for den daglige efterlevelse af informationssikkerhedskravene, samt for formidling af informationssikkerhed til medarbejdere, konsulenter og andre relevante samarbejdspartnere og kontrahenter i eget ansvarsområde.

Direktører med procesansvar
Den fagansvarlige direktør er ansvarlig for, at der findes beskrevne, manuelle forretningsgenoprettelsesplaner (Business Continuity Plans - BCP) og/eller instrukser, dækkende for egne forretningsprocesser samt sikre klassificering af disse.

Direktør for IT
Den ansvarlige direktør for Bankens IT, har ansvaret for at sikre efterlevelsen af den gældende Informationssikkerhedspolitik og dertilhørende informationssikkerhedskrav, herunder i de valgte teknologier, IT-løsninger og ved de kritiske IT-leverandører.

Direktøren har ansvaret for løbende at overvåge de implementerede foranstaltninger, ved tilrettelæggelse og gennemførelse af egenkontroller for at sikre, at disse er designet korrekt, implementeret og er effektive.

Direktøren skal tillige sikre at IT-strategien lægger klare IT-sikkerhedsmålsætninger for nærværende politik gennem et fokus på IT-systemer, IT-tjenester, personale og processer.

Ansvarlig direktør for IT har også ansvar for at opdatere, vedligeholde og teste IT-beredskabsplan og IT-reetableringsprocedurer (Disaster Recovery Plans - DRP).

CISO (Chief Information Security Officer)
CISO'en er ansvarlig for at drive Bankens Informationsledelsessystem (ISMS), herunder årshjulet med de planlagte sikkerhedsaktiviteter (awareness, trussels-og risikovurderinger, rapportering m.m.).

CISO'en er ansvarlig for at følge op på informationssikkerhed og IT-risici i medfør af Ledelsesbekendtgørelsens bilag 5, herunder løbende at gennemføre kontrol med

overholdelse af Informationssikkerhedspolitikken, understøttende krav og -processer for informationssikkerhed.

Desuden er CISO'en ansvarlig for at opdatere og vedligeholde IT-beredskabsmålsætning på vegne af Bankens direktion og bestyrelse samt at efterprøve IT-beredskabsplanen minimum en gang årligt.

CISO'en rapporterer til direktionen og bestyrelsen periodisk, med minimum samme interval, som Risikoansvarliges risikorapportering.

Ansvaret inkluderer beføjelser til at foretage enhver form for undersøgelse omkring informationssikkerheden, 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 informationssikkerhed 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
Den fagansvarlige direktør er systemejer for egne, indkøbte IT-systemer, såvel interne, som eksterne, der anvendes i Banken - inklusive cloudløsninger. Systemejer skal, som minimum, have ansvar for:

- at systemet forretningsmæssigt er i overensstemmelse med de nødvendige forretningsbehov
- at systemet er compliant (overholder gældende regler) med gældende Informationssikkerhedspolitik og understøttende krav
- at der udarbejdes risikovurderinger på systemer
- at systemer og disses data, jf. model for dataklassifikation, klassificeres
- håndtering af revisionsrapporter, som vedrører det pågældende system
- 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
- løbende at overvåge de implementerede foranstaltninger, ved tilrettelæggelse og gennemførelse af egenkontroller for at sikre, at disse er designet korrekt, implementeret og er effektive.

IT-sikkerhedsudvalg
IT-sikkerhedsudvalget er af Bankens bestyrelsen bemyndiget til at træffe IT-relaterede beslutninger, som har indflydelse på Bankens IT-risici. Udvalget er samtidig rådgivende

og støttende for forretningen, på spørgsmål om informationssikkerhed og risikohåndtering.

Udvalget er ansvarligt for evaluering og styring af risikobilledet af væsentlige IT-risici. Desuden understøtter udvalget bankens arbejde med Informationssikkerhedspolitik og understøttende informationssikkerhedskrav. Udvalget er ligeledes bemyndiget til, på vegne af direktionen, at godkende nye og ændrede informationssikkerhedskrav.

Udvalget evaluerer og sikrer godkendelse af dispensationer fra manglende overholdelse af Informationssikkerhedspolitikken og understøttende informationssikkerhedskrav, herunder forvalter et samlet register for dispensationer. Udvalget skal ligeledes rapportere på status for og på godkendte dispensationer til direktion og bestyrelse. Udvalget skal rapportere til direktionen om nye godkendelser, i forlængelse af bevilling af disse.

Business Continuity Manager (BCM)
Skal sikre efterlevelse af bankens målsætning for beredskab gennem afprøvning og udvikling af BCP'ere (Business Continuity Plans) samt samarbejde med forretning, IT og kritiske leverandører, og disses DRP'ere (Disaster Recovery Plans).
BCM skal endvidere rapportere til bankens ledelse på test og afprøvning af BCP'ere.

Medarbejder i banken
Den enkelte medarbejder er ansvarlig for minimum en gang om året at gøre sig bekendt med og løbende efterleve Informationssikkerhedspolitik og understøttende informationssikkerhedskrav, for dennes arbejdsområde.

Principper for implementering af politikken i uddybende informationssikkerhedskrav og procedurer

Spar Nord IT og relevante forretningsområder har ansvaret for at udarbejde processer i det omfang, det er nødvendigt, til operationalisering af Informationssikkerhedspolitikken. IT-sikkerhed, som 2. forsvarslinje rådgiver om krav til informationssikkerhed og IT-sikkerhedsforanstaltninger. Funktionen skal være bekendt med de IT-sikkerhedsforanstaltninger, der anvendes til imødegåelse af risici.

Efterlevelse

Banken anvender funktionsadskillelsesprincipperne om de tre linjer til at sikre, at Informationssikkerhedspolitikken efterleves, og at IT operationelle risici håndteres og overvåges. Dette sker igennem følgende funktioner i Banken:

Linje	1. linje	2. linje	3. linje
Funktion	Risiko ejerskab	Målsætning og kontrol	Efterlevelse
Ansvar & opgaver	1: Ansvarlig for gennemførsel af risikostyringsaktiviteter. 2: Supportere forretningen ved at udarbejde processer og facilitere risikoprocessen.	1: Definere krav og overordnede metodevalg. Følge op og rapportere på overholdelse af Informationssikkerhedspolitikken Opfølgning på udarbejdede rapportering. Påse at risikostyringsprocesser fungerer tilfredsstillende. 2: At føre tilsyn med, at banken tilrettelægger sine IT-processer med henblik på overholdelse af gældende lovgivning.	1: Udfører revision med henblik på, at sikre efterlevelse af lovgivning.
Placering	1: "Forretningen", Procesejere og Systemejere 2: Spar Nord IT	1: IT-Risikostyringsfunktionen 2: Compliance	1: Intern revision

1. Linje udgøres af linjeorganisationen og særligt de organisatoriske funktioner, som arbejder med behandling af informationer og teknologi. Denne linje er ansvarlige for at identificere, vurdere og håndtere risici, når de identificeres.

2. Linje udgøres primært af Risikostyringsfunktionen, som overvåger overholdelse af IT-sikkerheds-niveauet og risikoniveauet for operationelle IT-risici, i overensstemmelse med Risikostyringens funktionsbeskrivelse. Complianceafdelingen overvåger og kontrollerer for overholdelse af gældende lovgivning for den finansielle sektor.

3. Linje udgøres af Intern Revision, der har ansvaret for at udføre uafhængig revision af den samlede håndtering af risici og de interne kontroller i Banken – samt rapportere om sit arbejde til bestyrelsen.

4. Styring af IT-risici

Bankens eksponering overfor operationelle IT-risici skal ske i overensstemmelse med politikken for IT-risikostyring og politikken for operationelle risici.
IT-Sikkerhed har ansvaret for at assistere organisationen med identifikation af IT-risici, vurdering af kontrolforanstaltninger og kontroller.

Sammenhæng mellem Informationssikkerhedspolitikken og IT-risikostyringspolitikken

Bestyrelsen har besluttet, at Bankens IT-sikkerhedsstyring skal være risikobaseret, og at Informationssikkerhedspolitikken således skal medvirke til at holde IT-risici på et niveau, som er acceptabelt for bestyrelsen. Dette skal ske ved, at Banken udarbejder en samlet, overordnet risikovurdering, som skal anvendes til opdatering af Informationssikkerhedspolitikken og sikring af, at Informationssikkerhedspolitikken tager højde for det aktuelle risikobillede.

5. Outsourcing

Ved outsourcing og videreoutsourcing til eksterne leverandører, skal IT-sikkerhedsniveauet for Banken opretholdes. Dette er ensbetydende med, at sikkerhedsprincipperne i Informationssikkerhedspolitikken skal efterleves. Enhver outsourcing af væsentlige eller ikke-væsentlige aktivitetsområder, skal følge reglerne i outsourcing-politikken og skal registreres centralt, for at der løbende kan føres kontrol med leverandørernes IT-sikkerhedsniveau.

Forhold vedr. kritiske og strategiske IT-leverandører

I overensstemmelse med kravene i Bekendtgørelse om outsourcing for kreditinstitutter m.v., har bestyrelsen ved beslutning om outsourcing af dele af IT-driften sikret, at leverandørerne har den evne og kapacitet, der er nødvendig for at kunne varetage de outsourcede opgaver på en tilfredsstillende måde og herunder har de tilladelser, der efter den relevante lovgivning for IT-området er foreskrevet.
Banken skal sikre overvågning af, at leverandørerne overholder relevant lovgivning på området. Banken benytter sig i den forbindelse af årlige erklæringer fra datacentralens eksterne og interne systemrevision.

Banken skal udarbejde interne regler, som sikrer, at leverandørens opgavevaretagelse foregår betryggende. Reglerne indeholder procedurer for, hvorledes Banken sikrer sig, at leverandøren lever op til forpligtelserne i kontrakten og rapportering til bestyrelsen, således at bestyrelsen har indsigt i, om aktiviteterne udføres tilfredsstillende.

Sammenhæng mellem Informationssikkerhedspolitikken og politikken for outsourcing af aktivitetsområder

IT-risici, der relaterer sig til brugen af outsourcing, skal inddrages i IT-risikostyringen, og skal rapporteres på lige fod med andre risici. Herudover skal det sikres, at relevante foranstaltninger, til at imødekomme risici, identificeret i relation til outsourcede

aktiviteter, indarbejdes i aftaler med outsourcing leverandører, og at effektiviteten heraf løbende overvåges og kontrolleres, jf. politikken for outsourcing af aktivitetsområder.

6. Sikkerhedsprincipper

Informationssikkerhedspolitikken skal understøttes af en række sikkerhedsprincipper, som skal uddybes i supplerende krav og procedurer. De vigtigste principper for overholdelse af denne politik beskrives i nedenstående afsnit.

6.1 Beredskab og forretningskontinuitet

Direktionen skal sikre, at der udarbejdes en IT-beredskabsplan. Planen skal udarbejdes på baggrund af forretningskonsekvensanalyser, og skal indeholde målsætning for genetablering af normal drift i tilfælde af fejl, nedbrud, tab af data eller systemer, samt hel eller delvis ødelæggelse af bygninger, maskinel og kommunikationsveje, i overensstemmelse med bestyrelsens målsætning for IT-beredskab.

Direktionen skal sikre, at der løbende tages stilling til nødvendig redundans og flercenterdrift, for at sikre opretholdelsen af Bankens væsentligste funktioner.

Målsætningen for Bankens beredskabsplanlægning er, at kritiske, forretningsmæssige IT-løsninger kan retableres og anvendes af et begrænset antal medarbejdere fra midlertidige lokaler, indenfor målsætningen som nævnt i Målsætning for IT-Beredskab, efter at beslutning om iværksættelse af beredskabsplanen er truffet, hvilket benævnes nøddrift.

IT-Beredskabsplanen skal understøtte Bankens behov og målsætning, om tidsfrister for genoptagelse til normal drift. Ved udarbejdelsen af IT-beredskabsplanen, skal Banken inddrage andre relevante beredskabsplaner, herunder Bankens forretningskontinuitetsplaner samt genopretningsplaner fra kritiske systemleverandører.

Perioden for nøddrift skal planlægges i overensstemmelse med målsætningen for IT-beredskab, hvorefter der skal være fuld kapacitet til rådighed. I denne periode, kan der blive tale om at reducere åbningstiden på udvalgte systemer, indtil der er sikkerhed for, at alle daglige rutiner er genetableret.

Direktionen skal sikre, at beredskabsplaner regelmæssigt afprøves. Omfanget af afprøvningerne skal gennemføres med afsæt i relevante scenarier og Bankens trusselsbillede. Direktionen skal rapportere væsentlige resultater fra beredskabstestene til bestyrelsen.

Direktionen skal sikre at, beredskabsplanerne, aktivitetsplanerne og genopretningsprocedurer løbende og mindst en gang årligt opdateres på baggrund af testresultater, trussels- og risikovurderinger.

Disse beredskabsplaner skal være understøttet af relevante forretningskontinuitets- (BCP) og genopretningsplaner (DRP).

6.2 Medarbejdere, samarbejdspartnere og kontrahenter

Det skal sikres, at Bankens medarbejdere, samarbejdspartnere og kontrahenter er egnede til de roller de bestrider, ved at være bevidste om efterlevelsen af deres informationssikkerhedsansvar.

Banken skal sikre sine IT-aktiver og systemadgange ved ændringer eller ophør til ansættelsesforhold og samarbejdsaftaler.

Der skal kommunikeres krav for accepteret brug af IT, hvori ansvaret gøres bekendt. Kravene skal som minimum indeholde følgende emner:

Medarbejdere:

- Processer for indrapportering af informationssikkerhedshændelser
- Forhold vedr. anvendelse og hemmeligholdelse af personlige passwords
- Brug af e-mail, herunder opmærksomhed på mailphishing, CEO-fraud og ransomware
- Databehandling af fortrolige kundedata (i og udenfor Banken)
- Anvendelse af mobilt udstyr (hjemmearbejde og under transport)
- Sanktioner ved misligholdelse af brugeransvaret

Samarbejdspartnere og kontrahenter:

- Fortrolighedserklæring
- Procedure for indrapportering af informationssikkerhedshændelser
- Brug af e-mail, herunder opmærksomhed på mailphishing, CEO-fraud og ransomware
- Forhold vedr. anvendelse og hemmeligholdelse af personlige passwords
- Sanktioner ved misligholdelse af brugeransvaret

6.3 Driftsafvikling

Driftsleverancer varetages af Bankens egen IT-afdeling samt eksterne driftsleverandører. Det kræves, at disse til enhver tid har tilstrækkelige IT-ressourcer til at opretholde en sikker og stabil drift i henhold til den indgået driftsaftale. Tillige kræves det, at disse også råder over kompetent personale, maskinel, faciliteter samt nødvendige kapabiliteter, til løbende at imødegå og bekæmpe cyberangreb.

Det kræves, at driftsleverandøren har procedurer for hændelses- og ændringsstyring og problemstyring, at IT-risici identificeres, vurderes og håndteres, og indgår som datakilder i Bankens egen risikostyringsproces. Driften skal afvikles i overensstemmelse med de i denne Informationssikkerhedspolitik angive krav, samt underbyggende metodebeskrivelser, politikker, regler og procedurer.

Det kræves at hændelser kan klassificeres efter væsentlighed, således at Banken kan sikre den rette håndtering samt efterleve rapporteringsforpligtigelser ved væsentlige hændelser.

Det kræves, at Bankens forbindelser til netværk skal være beskyttet mod uautoriseret adgange fra eksterne brugere, og at systemleverandøren har tilvejebragt betryggende sikring mod indtrængning i Bankens interne netværk.

Det kræves, at brug af privilegerede adgangsrettigheder, brugernes anvendelse af systemløsninger samt øvrige hændelser i systemløsninger logges i nødvendigt og tilstrækkeligt omfang, og i henhold til den afdækkede risiko.

Der skal løbende føres kontrol med leverandørernes efterlevelse af principperne for driftsafvikling samt jf. Outsourcing-politikkens bestemmelse om 'løbende forvaltning og kontrol'.

6.4 Beskyttelse og håndtering af IT-aktiver

Det kræves at væsentligheden af IT-aktiver kan udledes på baggrund af understøttelse af Bankens forretningsprocesser. Derfor skal det sikres, at der udpeges en ejer af IT-aktiver og at disse kan identificeres efter anvendelse og klassifikation, og tilsvarende beskyttes mod fysiske og logiske trusler. Dette gælder særligt for cybertrusler og trusler, som kan medføre fejl på IT-aktiverne, der giver betydelige konsekvenser for Bankens kunder, medarbejdere og samarbejdspartnere.

IT-aktiver skal sikres imod uautoriseret adgang, ændring, fjernelse og destruktion af data, lagret på medier. Risikovurderinger skal anvendes for at afdække, hvorvidt IT-aktiver beskyttes i betryggende omfang i forhold til Bankens risikotolerance.

6.5 Backup og sikkerhedskopiering

Det skal sikres, at sikkerhedskopiering af væsentlige (skal defineres jf. gældende data- og systemklassifikationsmodel) data, skal foregå efter fastlagte regler, der indeholder krav om periodisk afprøvning og opbevaring af en kopi under betryggende forhold, for at beskytte Banken mod tab af data.

Det skal sikres at, hyppigheden for sikkerhedskopiering af systemer og data baseres på Bankens risikovurderinger, forretningskonsekvensanalyse (BIA), sammenhæng til planer for forretningskontinuitet, herunder datas kritikalitet og stillingtagen til principperne for Recovery Point Objective (RPO) og Recovery Time Objective (RTO).

Det skal sikres, at sikkerhedskopier skal opbevares sikkert og være utilgængelige for uautoriserede personer og brugere. Logisk og fysisk funktionsadskillelse skal sikres omkring backupmiljøet således, at ingen kan have adgang til samtlige kopier af data.

Det kræves, at systemleverandørene kan dokumentere ovenstående krav om backup- og sikkerhedskopiering via løbende rapportering af kontrolaktiviteter og årlig revisionserklæring.

6.6 Adgange til informationer og systemer

Det kræves at adgange til informationer og systemer styres efter dokumenterede procedurer, som bl.a. tager hensyn til principper for funktionsadskillelse i afsnit 6.10 således, at kundeadgange på kundevendte applikationer ikke er omfattet.

Det skal sikres, at adgangsrettigheder alene tildeles i et omfang, det er nødvendigt og relevant for, at den enkelte medarbejder kan løse sine konkrete arbejdsopgaver.

Alle tildelinger og ændringer af adgange til systemer og data skal udføres centralt og af særligt betroet medarbejdere. Anmoder- og godkendelsesfunktionen skal være funktionsadskilt, og alle anmodninger skal dokumenteres og opbevares så de efterfølgende kan anvendes for revision og opfølgning.

Alle brugeradgange skal være personhenførbare og anvende entydig brugeridentifikation.

Det kræves, at der er procedurer for logning af brugeraktivitet. Det skal således sikres, at logning foretages risikobaseret, med det formål at kunne opdage og efterforske uregelmæssige aktiviteter. Logdata skal sikres mod manipulation under både transport og opbevaring.

Tildeling af privilegerede adgangsrettigheder skal begrænses til et absolut og tidsbegrænset minimum, og brugen heraf skal logges særligt og overvåges for eventuel misbrug. Det skal alene være nærmeste chef/direktør der kan godkende privilegerede adgangsrettigheder og med indsigt i det arbejdstinget behov. Det skal sikres, at der kvartalsvist foretages opfølgning af systemadgange og rettigheder.

6.7 Systemudvikling og vedligeholdelse af forretningsapplikationer

Ved al udvikling af forretningsapplikationer skal det sikres, at udviklingsaktiviteterne er af den ønskede kvalitet og sikkerhedsstandard, ved deltagelse i nødvendige testaktiviteter, styregrupper og øvrige fora.

Det kræves, at systemleverandøren, intern som ekstern, følger anerkendte standarder og benytter minimum tre miljøer ved udvikling af nye forretningssystemer (drifts-, test- og udviklingsmiljø) samt et dokumenteret ændrings- og idriftsætningssystem.

Ved kritiske systemkomponenter, der er tilkoblet til internettet, skal det være et krav, at der gennemføres en tilfredsstillende sårbarhedsscanning forud for ibrugtagningen. Bankens internetvendte og egenudviklede applikationer skal altid være resiliente overfor det aktuelle trusselsbillede.

Det kræves, at alle idriftsættelser eller ændringer i systemer skal foretages efter en kontrolleret og dokumenteret proces, som systemleverandøren ejer og er forpligtet til at anvende.

Det kræves, at der forefindes en procedure for testaktiviteter, der sikrer datas fortrolighed, og integritet efter disses klassifikation.

6.8 Projektstyring

Informationssikkerhed skal integreres i projektmodeller og som et fast element i gennemførelsen af projekter. Det skal sikres, at alle informationsrisici, ved gennemførelsen af projekter, identificeres, analyseres og håndteres herunder, at informationer, der håndteres i projekter, klassificeres, og at der implementeres foranstaltninger til at beskytte fortroligheden, integriteten og tilgængeligheden af disse samt af de systemer og applikationer, som anvendes til behandling.

Det kræves at informationssikkerheden opretholdes i den fulde levetid for projekter og at risici og imødekommende foranstaltninger løbende verificeres og evalueres.

6.9 Risikovurdering

Den fastlagte metode til risikovurderinger fra IT-risikostyringspolitikken skal anvendes. Der skal gennemføres risikovurderinger af kritiske IT-aktiver i en kontinuerlig proces, til at identificere væsentlige risici, og til fastlæggelse af nødvendige sikkerhedsforanstaltninger.

6.10 Funktionsadskillelse

Funktionsadskillelse skal implementeres og overvåges i tilstrækkeligt omfang, til at sikre, at risikoen for enkelte funktioner eller personer, der udfører væsentlige handlinger, som kan kompromittere sikkerheden, minimeres.
Det skal sikres, at der er overordnet adskillelse mellem funktioner og personer på tværs af områderne:

- Systemudvikling
- Test
- Systemdrift
- Forretningsaktiviteter

Forretningssystemer skal designes med fuldstændig adskillelse mellem forretningsbrugere og administrations- og operatørbrugere.

6.11Awareness

Der skal sikres løbende information og uddannelse til Bankens medarbejdere omkring informationssikkerhed og beskyttelse af persondata, for at sikre en effektiv sikkerhedskultur. Der skal foretages vurdering om målrettet informationssikkerhedstræning for medarbejdere, som er i berøring med risikofyldte aktiviteter.

6.12 Brud på Informationssikkerhedspolitikken og informationssikkerhedskrav

Det skal sikres, at alle medarbejdere nemt kan rapportere hændelser, der har konsekvens for informationssikkerheden, og er informeret om deres ansvar hertil. Hændelserne skal rapporteres til Spar Nord IT, der afgør om, hvorvidt hændelsen straks skal rapporteres til direktionen.

Bestyrelsen skal orienteres om væsentlige brud på Informationssikkerhedspolitikken, ligesom øvrige relevante interessenter.

6.13 Sanktionering ved brud på politikken

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.

7. Rapportering, kontrol og opfølgning

Bestyrelsen skal orienteres om væsentlige informationssikkerhedshændelser. Orienteringen skal ske løbende, dog mindst en gang årligt i forbindelse med ajourføring af politikken. Hændelser af væsentlig karakter skal rapporteres tydelig og rettidigt til bestyrelsen og direktionen, samt til øvrige samarbejdspartnere, herunder særligt Finanstilsynet og Center for Cybersikkerhed.

Direktionen skal sikre, at der etableres overvågning og kontrol med efterlevelse af Informationssikkerhedspolitikken, og løbende rapportere til bestyrelsen, om manglende overholdelse heraf. Det kræves, at effektiviteten af de iværksatte foranstaltninger verificeres ved uafhængige gennemgange og valideres ved gennemførelse af tekniske test. Resultaterne af de udførte gennemgange og tests, skal indgå i rapportering vedrørende efterlevelse af Informationssikkerhedspolitikken og i vurderingen og rapporteringen af IT-risikoeksponeringen.

8. Dispensationer fra politikken

Direktionen kan, såfremt forholdene nødvendiggør det, give dispensation fra Informationssikkerhedspolitikkens anvisninger og krav. Dispensationerne skal løbende overvåges og risikovurderes.

Det kræves at dispensationer fra Informationssikkerhedspolitikken skal rapporteres periodisk til bestyrelsen. Eventuelle dispensationer skal dokumenteres og opbevares i centralt register for dispensationer, og skal forvaltes af bankens IT-sikkerhedsudvalg.

9. Godkendelse af politikken

Informationssikkerhedspolitikken træder i kraft ved bestyrelsens godkendelse 1. juli 2023 og erstatter den hidtil gældende Informationssikkerhedspolitik.

Referencer til øvrige dokumenter

Interne, aktuelle:

a) Risikovurdering til revidering af Informationssikkerhedspolitik
b) IT-Strategi
c) IT-sikkerhedskrav
d) Politik for outsourcing af aktivitetsområder
e) Politik for operationel risikostyring
f) Politik for IT-risikostyring
g) Politik for Datagovernance- og Databeskyttelsespolitik
h) Målsætning for IT-Beredskab
i) Lovpligtig redegørelse for dataetik 1

Eksterne:

j) Gældende informationssikkerhedsstandard, ISO/IEC 27001 – Appendiks A og ISO/IEC 27002:2022
k) Bekendtgørelse om ledelse og styring af pengeinstitutter m.fl., BEK nr. 1254 af 11/06/2021, Bilag 5 IT-strategi, IT-risikostyringspolitik og IT-sikkerhedspolitik

1.

BILAG – Mapning imellem Informationssikkerhedspolitikken og understøttende informationssikkerhedskrav

Informationssikkerhedspolitik	Informationssikkerhedskrav
1. Målsætning og dækning	5.1 Politikker og informationssikkerhed 5.14 Overførsel af information 5.31 Juridiske. Lovmæssige, regulatoriske og kontraktlige krav
2. Sammenhæng mellem IT-risikoprofil og Bankens sikkerhedsniveau	5.31 Juridiske. Lovmæssige, regulatoriske og kontraktlige krav 5.33 Beskyttelse af optegnelser 5.36 Overensstemmelse med politikker, regler og standarder for informationssikkerhed
3. Organisation og ansvar	5.2 Roller og ansvar for informationssikkerhed 5.4 Ledelsens ansvar 6.1 Screening (Baggrundstjek af medarbejdere) 6.2 Ansættelsesvilkår og -betingelser 6.5 Ansvar i forbindelse med ophør eller ændring af ansættelsesforhold
4. Styring af IT-risici	5.21 Styring af informationssikkerhed i IKT-forsyningskæden 5.31 Juridiske. Lovmæssige, regulatoriske og kontraktlige krav 5.33 Beskyttelse af optegnelser 8.8 Styring af tekniske sårbarheder
5. Outsourcing	5.19 Informationssikkerhed i leverandørforhold 5.20 Håndtering af informationssikkerhed i leverandøraftaler 5.21 Styring af informationssikkerhed i IKT-forsyningskæden 5.22 Overvågning, vurdering og ændringsstyring af leverandørydelser 5.31 Juridiske. Lovmæssige, regulatoriske og

	kontraktlige krav 5.32 Intellektuelle ejendomsrettigheder 5.33 Beskyttelse af optegnelser 6.3 Awareness, uddannelse og træning vedrørende informationssikkerhed 6.5 Ansvar i forbindelse med ophør eller ændring af ansættelsesforhold 6.6 Hemmeligholdelses- og fortrolighedsaftaler 8.30 Outsourcet udvikling 8.31 Adskillelse af udviklings-, test- og produktionsmiljøer
6. Sikkerhedsprincipper	5.3 Funktionsadskillelse 5.36 Overensstemmelse med politikker, regler og standarder for informationssikkerhed
6.1 Beredskab og forretningskontinuitet	5.30 IKT-parathed til understøttelse af business continuity 8.14 Redundans i faciliteter til informationsbehandling
6.2 Medarbejdere og samarbejdspartnere	5.10 Acceptabel brug af information og understøttende aktiver 5.14 Overførsel af information 5.15 Administration af adgange 5.19 Informationssikkerhed i leverandørforhold 5.20 Håndtering af informationssikkerhed i leverandøraftaler 5.24 Planlægning og forberedelse af incidenthåndtering ved sikkerhedsincidents 5.31 Juridiske. Lovmæssige, regulatoriske og kontraktlige krav 5.32 Intellektuelle ejendomsrettigheder 5.33 Beskyttelse af optegnelser 6.1 Screening (Baggrundstjek af medarbejdere) 6.2 Ansættelsesvilkår og -betingelser 6.3 Awareness, uddannelse og træning vedrørende informationssikkerhed 6.5 Ansvar i forbindelse med ophør eller

	ændring af ansættelsesforhold 6.6 Hemmeligholdelses- og fortrolighedsaftaler 6.7 Distancearbejde 8.15 Logning 8.18 Brug af privilegerede understøttende programmer
6.3 Driftsafvikling	5.14 Overførsel af information 5.15 Administration af adgange 5.23 Informationssikkerhed ved brug af cloudtjenester 5.29 Informationssikkerhed under driftsforstyrrelse 5.31 Juridiske. Lovmæssige, regulatoriske og kontraktlige krav 5.33 Beskyttelse af optegnelser 5.35 Uafhængig vurdering af informationssikkerhed 5.37 Dokumenterede driftsprocedurer 8.6 Kapacitetsstyring 8.9 Konfigurationsstyring 8.17 Synkronisering af ure 8.18 Brug af privilegerede understøttende programmer 8.19 Softwareinstallation i test- og produktionssystemer 8.20 Netværkssikkerhed 8.21 Sikring af netværkstjenester 8.22 Segmentering af netværk 8.23 Webfiltrering 8.24 Brug af kryptografi 8.26 Krav til applikationssikkerhed 8.29 Sikkerhedstest under udvikling og godkendelse 8.31 Adskillelse af udviklings-, test- og produktionsmiljøer 8.32 Ændringsstyring 8.33 Information til brug for test 8.34 Beskyttelse af informationer under audit

6.4 Beskyttelse og håndtering af IT-aktiver	5.9 Fortegnelse over information og understøttende aktiver 5.11 Returnering af aktiver 5.12 Klassifikation af information 5.19 Informationssikkerhed i leverandørforhold 5.31 Juridiske. Lovmæssige, regulatoriske og kontraktlige krav 5.32 Intellektuelle ejendomsrettigheder 5.33 Beskyttelse af optegnelser 6.6 Hemmeligholdelses- og fortrolighedsaftaler 7.1 Fysisk områdesikring 7.2 Fysisk adgangskontrol 7.3 Sikring af kontorer, lokaler og faciliteter 7.4 Fysisk sikkerhedsovervågning 7.5 Beskyttelse mod fysiske og miljømæssige trusler 7.6 Arbejde i sikre områder 7.7. Ryddet skrivebord og låste skærme 7.8 Placering og beskyttelse af udstyr 7.9 Sikring af aktiver uden for organisationens områder 7.10 Lagringsmedier 7.11 Forsyningssikkerhed 7.12 Sikring af kabler 7.13 Vedligeholdelse af udstyr 7.14 Sikre bortskaffelse eller genbrug af udstyr 8.1 Brugerenheder 8.6 Kapacitetsstyring 8.7 Beskyttelse mod malware 8.8 Styring af tekniske sårbarheder 8.10 Sletning af information 8.11 Datamaskering 8.12 Forebyggelse af datalækage 8.14 Redundans i faciliteter til informationsbehandling 8.15 Logning 8.16 Overvågning af aktiviteter 8.18 Brug af privilegerede understøttende programmer 8.19 Softwareinstallation i test- og

	produktionssystemer 8.20 Netværkssikkerhed 8.21 Sikring af netværkstjenester 8.22 Segmentering af netværk 8.23 Webfiltrering 8.24 Brug af kryptografi 8.26 Krav til applikationssikkerhed 8.33 Information til brug for test 8.34 Beskyttelse af informationer under audit
6.5 Backup og sikkerhedskopiering	5.12 Klassifikation af information 5.23 Informationssikkerhed ved brug af cloudtjenester 5.31 Juridiske. Lovmæssige, regulatoriske og kontraktlige krav 5.33 Beskyttelse af optegnelser 8.7 Beskyttelse mod malware 8.10 Sletning af information 8.12 Forebyggelse af datalækage 8.13 Backup af information 8.14 Redundans i faciliteter til informationsbehandling 8.20 Netværkssikkerhed 8.21 Sikring af netværkstjenester 8.22 Segmentering af netværk 8.23 Webfiltrering 8.24 Brug af kryptografi
6.6 Adgange til informationer og systemer	5.13 Mærkning af information 5.14 Overførsel af information 5.15 Administration af adgange 5.16 Styring af identifikation 5.17 Autentifikationsoplysninger 5.18 Adgangsrettigheder 5.23 Informationssikkerhed ved brug af cloudtjenester 5.31 Juridiske. Lovmæssige, regulatoriske og kontraktlige krav 5.33 Beskyttelse af optegnelser

	5.34 Privatlivsbeskyttelse og beskyttelse af personoplysninger 6.1 Screening (Baggrundstjek af medarbejdere) 6.2 Ansættelsesvilkår og -betingelser 6.5 Ansvar i forbindelse med ophør eller ændring af ansættelsesforhold 6.6 Hemmeligholdelses- og fortrolighedsaftaler 6.7 Distancearbejde 8.2 Privilegerede adgangsrettigheder 8.3 Begrænset adgang til information 8.4 Adgang til kildekode 8.5 Sikker autentifikation 8.7 Beskyttelse mod malware 8.11 Datamaskering 8.12 Forebyggelse af datalækage 8.14 Redundans i faciliteter til informationsbehandling 8.15 Logning 8.16 Overvågning af aktiviteter 8.18 Brug af privilegerede understøttende programmer 8.19 Softwareinstallation i test- og produktionssystemer 8.20 Netværkssikkerhed 8.21 Sikring af netværkstjenester 8.22 Segmentering af netværk 8.23 Webfiltrering 8.24 Brug af kryptografi 8.33 Information til brug for test 8.34 Beskyttelse af informationer under audit
6.7 Systemudvikling og vedligeholdelse af forretningsapplikationer	5.23 Informationssikkerhed ved brug af cloudtjenester 5.32 Intellektuelle ejendomsrettigheder 5.35 Uafhængig vurdering af informationssikkerhed 5.36 Overensstemmelse med politikker, regler og standarder for informationssikkerhed 6.6 Hemmeligholdelses- og fortrolighedsaftaler 8.11 Datamaskering 8.14 Redundans i faciliteter til

	informationsbehandling 8.15 Logning 8.16 Overvågning af aktiviteter 8.18 Brug af privilegerede understøttende programmer 8.19 Softwareinstallation i test- og produktionssystemer 8.20 Netværkssikkerhed 8.21 Sikring af netværkstjenester 8.22 Segmentering af netværk 8.23 Webfiltrering 8.24 Brug af kryptografi 8.25 Sikker udviklingslivscyklus 8.26 Krav til applikationssikkerhed 8.27 Sikker systemarkitektur og udviklingsprincipper 8.28 Sikker programmering 8.29 Sikkerhedstest under udvikling og godkendelse 8.30 Outsourcet udvikling 8.31 Adskillelse af udviklings-, test- og produktionsmiljøer 8.32 Ændringsstyring 8.33 Information til brug for test 8.34 Beskyttelse af informationer under audit
6.8 Projektstyring	5.8 Informationssikkerhed i projekter
6.9 Risikovurdering	- IT-Risikostyringspolitikken - Politik for Operationel sikkerhed
6.10 Funktionsadskillelse	5.3 Funktionsadskillelse 8.31 Adskillelse af udviklings-, test- og produktionsmiljøer
6.11 Awareness	5.34 Privatlivsbeskyttelse og beskyttelse af personoplysninger 6.3 Awareness, uddannelse og træning vedrørende informationssikkerhed

6.12 Brud på IT-sikkerhedspolitikken og IT-sikkerhedskrav	5.7 Underretning om trusler 5.24 Planlægning og forberedelse af incidenthåndtering ved sikkerhedsincidents 5.25 Vurdering af og beslutning om informationssikkerhedshændelser 5.26 Håndtering af informationssikkerhedsincidents 5.27 Læring af informationssikkerhedsincidents 5.28 Indsamling af bevismateriale 5.29 Informationssikkerhed under driftsforstyrrelse 6.4 Sanktioner 6.8 Indrapportering af informationssikkerhedshændelser 8.15 Logning
7. Rapportering, kontrol og opfølgning	5.5 Kontakt til myndigheder 6.8 Indrapportering af informationssikkerhedshændelser
8. Dispensationer fra politikken	- Proces for dispensationer for manglende overholdelse af Informationssikkerhedspolitik og understøttende informationssikkerhedskrav i HOPEX
9. Godkendelse af politikken	N/A