Lovtidende A

2019

Udgivet den 9. juli 2019

8. juli 2019. Nr. 710.

Bekendtgørelse om ændring af bekendtgørelse om ledelse og styring af pengeinstitutter m.fl.

§ 1

I bekendtgørelse nr. 1026 af 30. juni 2016 om ledelse og styring af pengeinstitutter m.fl., som ændret ved bekendtgørelse nr. 461 af 9. maj 2018, foretages følgende ændringer:

1. Bekendtgørelsens *indledning* affattes således:

»I medfør af § 65, stk. 2, § 70, stk. 7, § 71, stk. 3 § 152, stk. 2, og § 373, stk. 4, i lov om finansiel virksomhed, jf. lovbekendtgørelse nr. 457 af 24. april 2019, som ændret ved lov nr. 552 af 7. maj 2019, og § 21 og § 39, stk. 3, i lov om realkreditlån og realkreditobligationer m.v., jf. lovbekendtgørelse nr. 1188 af 19. september 2018, fastsættes:«

2. *§ 4, stk. 2, nr. 6,* affattes således:

»6) It-sikkerhedspolitik og it-risikostyringspolitik, jf. bilag 5.«

3. *Bilag 5* affattes som bilag 1 til denne bekendtgørelse.

§ 2

Bekendtgørelsen træder i kraft den 1. september 2019.

Finanstilsynet, den 8. juli 2019

JESPER BERG

/ Anders Kragsnæs Balling

CQ000958

Erhvervsmin.,
Finanstilsynet, j.nr. 1912-0033

Bilag 1

»Bilag 5

Anvendelsesområde og definitioner

1) Dette bilag indeholder bestemmelser om de i bekendtgørelsen omhandlende forhold, der relaterer sig til it-området, herunder it-sikkerhedsstyring.

Bestyrelsens opgaver og ansvar

2) Bestyrelsen skal på baggrund af en risikovurdering beslutte en it-sikkerhedspolitik for virksomheden.

3) It-sikkerhedspolitikken skal ud fra den ønskede risikoprofil på it-området indeholde en overordnet stillingtagen til alle væsentlige forhold vedrørende it-sikkerheden. Hvad der er væsentligt afhænger bl.a. af virksomhedens størrelse samt omfanget og kompleksiteten af virksomhedens it-anvendelse.

Følgende forhold skal der, under hensyn til virksomhedens størrelse, kompleksitet, forretningsmodel og forretningsomfang, tages stilling til:

a) Organisering af it-arbejdet, herunder funktionsadskillelse mellem
   - systemudvikling/-vedligeholdelse
   - it-drift og
   - virksomhedens forretningsførelse.
b) Regelmæssige risikovurderinger.
c) Beskyttelse af systemer, data, maskinel og kommunikationsveje.
d) Systemudvikling og vedligeholdelse af systemer.
e) Driftsafvikling.
f) Logning og overvågning.
g) Funktionsadskillelse.
h) Backup og sikkerhedskopiering.
i) Målsætning for beredskabsplaner.
j) Kvalitetssikring.
k) Adgangsstyring.
l) Principper for implementering af politikken i uddybende retningslinjer, forretningsgange og instrukser.
m) Forholdsregler i tilfælde af brud på it-sikkerhedspolitik og sikkerhedsregler.
n) Overholdelse af relevant lovgivning.
o) Rapportering, kontrol og opfølgning.
p) Eventuelle dispensationer fra it-sikkerhedspolitikken.

4) Er virksomheden et SIFI eller et G-SIFI, skal it-sikkerhedspolitikken, jf. nr. 3, indeholde en stillingtagen til behovet for etablering af flercenterdrift på alle forretningskritiske it-systemer, jf. § 2, stk. 3.

5) Bestyrelsen skal regelmæssigt og mindst en gang årligt revurdere it-sikkerhedspolitikken på baggrund af en opdateret risikovurdering, herunder vurdere hvorvidt it-sikkerhedspolitikken er tilstrækkelig til at sikre, at de risici, som it-anvendelsen medfører og forventes at medføre, fremover er på et for virksomheden acceptabelt niveau.

6) It-sikkerhedspolitikken skal i videst muligt omfang være uafhængig af den anvendte teknologi.

Direktionens opgaver og ansvar

7) Direktionen skal sikre, at virksomhedens it-sikkerhedspolitik efterleves. Direktionen skal uddybe it-sikkerhedspolitikken i forretningsgange m.v., der understøtter, at
   a) ansvar, herunder ejerskab for it-processer og ressourcer, er placeret,
   b) funktionsadskillelsen løbende bliver overvåget og revurderet,
   c) der er kontrol med opretholdelse af det ønskede it-sikkerhedsniveau samt håndtering af eventuelle svagheder,
   d) systemer og data klassificeres og prioriteres, jf. nr. 19,
   e) kritiske systemer, data og tværgående afhængigheder løbende identificeres og risikovurderes, jf. nr. 19,
   f) systemer (både basis- og brugersystemer) og konfiguration (hardware) samt ændringer hertil dokumenteres,
   g) der er sikkerhedskopiering af systemer og data, herunder opbevaring af sikkerhedskopierne,
   h) der anskaffes tilstrækkelige it-ressourcer,
   i) systemudvikling, konfiguration og vedligeholdelse samt afprøvning af nye og ændrede systemer sker betryggende,
   j) der foretages tests og anden kvalitetssikring,
   k) der foretages ændringshåndtering og problemstyring,
   l) der sker adgangskontrol til systemer og data, jf. nr. 16-19,
   m) der er tilstrækkelig fysisk sikkerhed, herunder fysisk adgangskontrol,
   n) der er tilstrækkelige it-beredskabsplaner og test af it-beredskabet, jf. nr. 20-23, og
   o) der gennemføres passende tiltag for at uddanne medarbejderne i it- og cybersikkerhed.

8) Direktionen skal sikre, at der etableres overvågning og kontrol med efterlevelsen af it-sikkerhedspolitikken.

9) Direktionen skal løbende rapportere til bestyrelsen om manglende overholdelse af it-sikkerhedspolitikken.

10) Er virksomheden et SIFI eller et G-SIFI, som har flere driftscentre, skal direktionen sikre, at afstanden mellem driftscentrene er tilstrækkelig til, at en hændelse, der sætter et driftscenter ud af drift, ikke kan ramme øvrige driftscentre samtidigt. Fastsættelse af en tilstrækkelig afstand mellem driftscentre skal foretages ud fra en konkret risikovurdering.

11) Direktionen i et penge- eller et realkreditinstitut, der af Finanstilsynet er udpeget som operatør af væsentlige tjenester, skal sikre, at Finanstilsynet og Center for Cybersikkerhed hurtigst muligt bliver underrettet om hændelser, som har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer. Underretningen skal indeholde oplysninger om antallet af brugere, som berøres af afbrydelse af den væsentlige tjeneste, hændelsens varighed, den geo-

grafiske udbredelse med hensyn til det område, der er berørt af hændelsen, og om eventuelle grænseoverskridende konsekvenser af hændelsen.

It-risikostyring, rettighedsstyring og beredskab

It-risikostyring

12) Bestyrelsen skal sikre, at virksomheden har en politik for it-risikostyring. Politikken kan være en særskilt politik eller indgå som en del af øvrige relevante politikker.

Politikken skal som minimum indeholde:
a) Mål for virksomhedens it-risikostyring.
b) Identifikation af, hvilke it-risici virksomheden kan være udsat for.
c) Stillingtagen til, hvorledes virksomhedens it-risici nedbringes til - eller fastholdes på et acceptabelt niveau.
d) Overordnede principper for it-sikkerhedsstyring, med henblik på at holde it-risici på et for bestyrelsen acceptabelt niveau.
e) Stillingtagen til:
   - risici knyttet til virksomhedens systemer og data
   - risici knyttet til integration og egnethed af virksomhedens it-systemer
   - it-risici knyttet til afhængighed af eksterne forhold, herunder underleverandører
   - it-risici knyttet til virksomhedens organisering, herunder manglende funktionsadskillelse.
f) Overordnede principper for, hvordan virksomheden skal registrere og kategorisere it-hændelser.
g) Overordnede principper for rapportering om it-hændelser til bestyrelsen, der skal sikre, at bestyrelsen til enhver tid har tilstrækkeligt indblik i virksomhedens it-risici og udviklingen heri.

13) Direktionen skal sikre, at virksomhedens it-risikostyringspolitik efterleves. Direktionen skal uddybe politikken i forretningsgange mv., der som minimum beskriver:
a) metoden for identifikation, vurdering og monitorering af it-risici
b) ansvarsplaceringen og organiseringen
c) etablering og implementering af kontrol- og sikringsforanstaltninger på baggrund af it-risici, samt hvordan der sikres sammenhæng mellem it-risici og kontroller
d) opfølgning på it-risici
e) rapportering til bestyrelsen af væsentlige it-risici.

14) Er virksomheden forpligtet til at have en risikostyringsfunktion og en risikoansvarlig efter § 16, indgår it-risikostyring som en del af den risikoansvarliges opgaver i overensstemmelse med bilag 7.

15) For fælles datacentraler gælder følgende:
a) Direktionen skal sikre, at virksomhedens it-risikostyring bliver varetaget på betryggende vis af en risikoansvarlig, som er udpeget af direktionen.
b) Direktionen skal sikre, at det tydeligt fremgår, hvilke opgaver og ansvarsområder i relation til it, den risikoansvarlige skal varetage.

c) Direktionen skal sikre, at den risikoansvarlige har adgang til alle relevante oplysninger i relation til it og har tilstrækkelige ressourcer.
d) Den risikoansvarlige skal have det samlede overblik over virksomheden og virksomhedens it-risici med henblik på at kunne vurdere, om der er en betryggende styring heraf.
e) Den risikoansvarlige skal sikre, at
   - alle væsentlige it-risici, identificeres, måles, håndteres og rapporteres korrekt
   - it-risici, der går på tværs af virksomhedens organisation, systemer og data, indgår i it-risikovurderingen
   - it-risici i outsourcede funktioner/opgaver indgår i vurderingen af virksomhedens samlede it-risikovurdering.

Rettighedsstyring

16) Direktionen skal sikre, at virksomheden har en betryggende risikobaseret bruger- og rettighedsstyring, som sikrer, at adgang til kritiske systemer og data kun sker ved et godkendt arbejdsbetinget behov.

17) Direktionen skal uddybe virksomhedens bruger- og rettighedsstyring i forretningsgange mv., der som minimum indeholder:
   a) identifikation og klassifikation af kritiske systemer og data i relation til rettighedsstyringen samt synliggørelse af risici herved
   b) identifikation af roller, rettigheder og kombinationer heraf samt synliggørelse af risici forbundet hermed, herunder i hvilket omfang adgangstildelingen, i medfør af et arbejdsbetinget behov, skal underlægges løbende kontrol og overvågning samt ansvaret herfor
   c) løbende kontrol og overvågning med anvendelsen af privilegerede og administrative adgange
   d) tildeling, ændring og rettidig fratagelse af adgange
   e) periodisk gennemgang af tildelte adgange, samt hvornår ikke godkendte adgange skal medføre kontrol- og opfølgningstiltag.

18) Direktionen skal sikre funktionsadskillelse i systemer og i tekniske miljøer på et dokumenteret grundlag.

19) Direktionen skal sikre, at systemer og data løbende klassificeres, kritiske adgange på tværs af systemerne identificeres, og at der etableres logning af kritiske systemadgange for at sikre en effektiv overvågning og rettidig sporing af uautoriseret aktivitet.

Beredskab

20) Direktionen skal sikre, at der udarbejdes en it-beredskabsplan, der indeholder 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, jf. nr. 3, litra i. I planen skal der, afhængig af virksomhedens forhold, være:
   a) en beskrivelse af, hvorledes der etableres en beredskabsorganisation, herunder rolle- og ansvarsfordelingen i beredskabsorganisationen
   b) aktivitetsplaner i forhold til alvorlige systemnedbrud, fejl og forstyrrelser i it-anvendelsen samt genopretningsprocedurer.

21) Direktionen skal sikre, at beredskabsplanen regelmæssigt afprøves. Omfanget af afprøvningerne skal bl.a. gennemføres med afsæt i relevante scenarier og virksomhedens trusselsbillede.

22) Direktionen skal rapportere væsentlige resultater for beredskabstestene til bestyrelsen.

23) Direktionen skal sikre, at beredskabsplanerne, aktivitetsplanerne og genopretningsprocedurer løbende og minimum en gang årligt opdateres på baggrund af testresultater, samt trussels- og risikovurderinger.«