

Sikkerhedshåndbog

2.0. Overordnede retningslinier for IT-sikkerheden

2.1. IT-sikkerhedspolitik

Indledning	IT-sikkerheden er en kritisk succesfaktor for e-nettet, og fokus på IT-sikkerhed har en central rolle i alle faser fra udvikling til drift af systemer i e-nettet.
Forretningsbeskrivelse	e-nettets formål er at opbygge, drive og vedligeholde et datanetværk, der skal sikre udveksling af strukturerede data mellem selskabets aktionærer indbyrdes og mellem aktionærerne og eksterne tilkoblede brugere samt med offentlige myndigheder.
Formål	Formålet med IT-sikkerhedspolitikken er at fastlægge e-nettets overordnede krav til IT-sikkerhed.
Anvendelse	IT-sikkerhedspolitikken skal anvendes som referenceramme i forbindelse med udarbejdelse af bl.a.: <ul style="list-style-type: none">• standarder• forretningsgange• procedurer - hvori der findes IT-sikkerhedsmæssige aspekter.
Målgruppe	Målgruppen er: <ul style="list-style-type: none">• alle ansatte i e-nettet• de leverandører, som e-nettet bruger i forbindelse med outsourcing mv.• de kunder, som benytter sig af e-nettets services.
Gyldighedsområde	e-nettets IT-sikkerhedspolitik vedrører alle aktiver, herunder al systemudvikling og databehandling uanset platform og om hele eller dele heraf er outsourcet eller lignende.
e-nettets opfattelse	IT-sikkerhed skal opfattes i videste forstand. Det vil sige, at det drejer sig for e-nettet om at beskytte programmer og data imod uønsket: <ul style="list-style-type: none">• afsløring• ændring• ødelæggelse• misbrug - uanset om årsagen er et hændeligt uheld eller en bevidst handling.
e-nettets krav	e-nettet skal sørge for bevarelse af systemernes funktionsevne både i forbindelse med mindre driftsforstyrrelser og i en katastrofesituation. Det fysiske IT-udstyr i e-nettet skal beskyttes mod tyveri, ødelæggelse

Sikkerhedshåndbog

	<p>eller misbrug.</p> <p>e-nettets image skal beskyttes ved at demonstrere kvalitet og kontinuitet i databehandlingen baseret på en professionel anvendelse af metoder og standarder og valg af løsninger med kvalitet (fx IT-sikkerhed).</p>
Overordnet målsætning	<p>Det er e-nettets målsætning, at der leveres en effektiv og pålidelig service, idet anvendelsen af IT er et bærende element i udøvelsen af e-nettets forretning. e-nettets service må ikke uden videre kunne påvirkes eller ødelægges af fejl, uheld eller forsætlige handlinger.</p>
<i>Mål</i>	<ul style="list-style-type: none">• e-nettet ønsker et datasikkerhedsniveau, der lever op til datasikkerhedsniveauet i finanssektoren.• Der skal opretholdes en høj grad af sikkerhed omkring de IT-registrerede informationers fortrolighed.• e-nettets IT-anvendelse skal leve op til lovgivningens krav.
<i>Risikobillede</i>	<p>e-nettets sikkerhed skal fastsættes, dels ud fra risikobilledet og dels ud fra de konsekvenser, som en given risiko eventuelt vil medføre, men sikkerhedsforanstaltninger skal afstemmes med forretningens krav til fleksibilitet, effektivitet og økonomi.</p>
<i>Ansvar</i>	<p>Det er ledelsens ansvar at målsætningen efterleves. Der må kun gives dispensation til sikkerhedspolitikken med direktionens tilladelse. Dispensationer af væsentlig betydning skal efterfølgende forelægges bestyrelsen.</p>
Beredskabsplans formål og målsætning	<p>Beredskabsplanens formål er,</p> <ul style="list-style-type: none">• at reducere kritiske og katastrofale situationers konsekvenser for e-nettets forretning• at sikre, at der på IT-området foreligger ajourførte planer og en organisation for håndtering af både pludselige og gradvist forværrede situationer• at roller og prioriteringer er kendt af alle, som har en rolle i planen <p>e-nettets beredskabsplan skal sikre, at</p> <ul style="list-style-type: none">• Kritiske administrative systemer er tilgængelige inden for 1 arbejdsdag (24 timer)• Realtidskundesystemer er tilgængelige indenfor 4 arbejdsdage (96 timer)• Ikke kritiske administrative- og øvrige kundesystemer er tilgængelige indenfor 7 arbejdsdage

Sikkerhedshåndbog

Sikkerhedsparametre:	<p>Ved etablering af sikkerhedsløsninger skal følgende indgå i overvejelserne:</p> <p><i>Konfidentialitet</i> Det skal sikres, at informationer ikke kommer til uvedkommendes kendskab, herunder skal aftale/brevhemmeligheden sikres. Endvidere skal lovgivningen vedr. persondata overholdes.</p> <p><i>Integritet</i> Det skal sikres, at indholdet af aftaler og data ikke forvanskkes. Konfidentialitet og integritet skal sikres såvel under transport af data som under lagring af data i systemerne.</p> <p><i>Tilgængelighed</i> Der skal etableres en driftssikkerhed med en service, som er tilgængelig, når kunderne har behov for den. Dækker også sikring mod systemhærværk, f.eks. i form af virusangreb eller fysisk ødelæggelse af IT-faciliteterne.</p> <p><i>Autenticitet</i> Det skal sikres, at brugeren er den, han udgiver sig for.</p> <p><i>Autorisation</i> Der skal etableres en sikker mekanisme til styringen af en genkendt brugers adgang til funktionalitet/data – altså det han/hun "må" få adgang til.</p> <p><i>Uafviselighed</i> Det skal kunne bevises, at en meddelelse er afsendt, henholdsvis modtaget, fx i de tilfælde der indgås økonomisk forpligtende aftaler.</p> <p><i>Sporbarhed</i> Det skal sikres, at man i en sags levetid kan finde tilbage og se, hvem der har gjort hvad og hvornår. Der skal altså opbevares et komplet transaktionsspor.</p>
Godkendelse	Direktionen fremlægger IT-sikkerhedspolitikken for bestyrelsen.
Ajourføring	e-nettet vil hver andet år foretage en vurdering af politikken for aktualitet og i givet fald foretage de fornødne rettelser og tilføjelser, som skal forelægges bestyrelsen til godkendelse, jf. afsnittet om godkendelse.
Referencer	Denne IT-sikkerhedspolitik er overordnet og er grundlæggende baseret på Standard of Good Practice fra Information Security Forum, som ligger meget tæt op af BS17799 :2005. Denne standard opdateres løbende.

Sikkerhedshåndbog

	<p>For en dybere gennemgang af de enkelte punkter henvises til ovennævnte Standard, som findes i e-nettet på engelsk.</p> <p>e-nettets IT-sikkerhedshåndbog fastlægger de detaljerede krav til IT-sikkerheden i e-nettet, realkreditinstitutter og leverandører.</p> <p>Der er etableret en sikkerhedsgruppe under e-nettet, hvor sikkerhedsspørgsmål diskuteres, løsninger beskrives og indstilles til gennemførelse.</p>
Kontrol	Ledelsen er ansvarlig for at kontrollere, at IT-sikkerhedspolitikken efterleves.