

FORSKRIFT OM BRUK AV INFORMASJONS- OG KOMMUNIKASJONSTEKNOLOGI (IKT)

Fastsatt av Kredittilsynet den 21. mai 2003 med hjemmel i lov 7. desember 1956 nr. 1 om tilsynet for kredittinstitusjoner, forsikringsselskaper og verdipapirhandel m.v. (Kreditttilsynsloven) § 4 nr. 2 og lov 17. november 2000 nr. 80 om børsvirksomhet § 3-4 første ledd annet punktum og lov av 17. desember 1999 nr. 95 om betalingsystemer § 3-3 første ledd annet punktum.

§ 1 Virkeområde

Forskriften gjelder for norske:

- 1. Forretningsbanker*
- 2. Sparebanker*
- 3. Finansieringsforetak*
- 4. Forsikringsselskaper*
- 5. Private, kommunale og fylkeskommunale pensjonskasser og pensjonsfond*
- 6. Børser og autoriserte markedsplasser*
- 7. Verdipapirforetak*
- 8. Forvaltningsselskaper for verdipapirfond*
- 9. Oppgjørssentraler*
- 10. Verdipapirregistre*
- 11. Inkassoforetak*
- 12. Eiendomsmeglerforetak*
- 13. E-pengeforetak*
- 14. Systemer for betalingstjenester*

Forskriften omfatter IKT-systemer som er av betydning for foretakets virksomhet. For eksterne brukere av foretakets IKT-systemer skal det foreligge avtaler som sikrer at forskriftens krav til sikkerhet og dokumentasjon ivaretas.

§ 2 Planlegging og organisering

Foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten. Det skal foreligge beskrivelse av den enkelte prosess og hvordan ansvaret for administrasjon, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en betryggende måte.

Ved utkontraktering av deler eller hele IKT-virksomheten skal foretaket ha egne retningslinjer som skal sikre leveransen.

Det skal oppnevnes en ansvarlig i foretaket for de ulike deler av IKT-virksomheten. Med ansvarlig menes en funksjon eller stilling.

§ 3 Risikoanalyse

Foretaket skal fastsette kriterier for akseptabel risiko forbundet med bruk av IKT-systemene. Foretaket skal ha en dokumentert prosess for gjennomføring av risikoanalyser av IKT-virksomheten. Prosessen skal blant annet definere klare ansvarsforhold og omfatte oppfølging av tiltak som iverksettes som et resultat av den gjennomførte risikoanalysen.

Foretaket skal minst en gang årlig, eller ved endringer som har betydning for IKT-sikkerheten, gjennomføre risikoanalyser for å påse at risiko styres innenfor akseptable grenser i forhold til foretakets virksomhet. Resultatet av risikoanalysen skal dokumenteres.

§ 4 Kvalitet

Foretaket skal fastsette kvalitetsmål for de enkelte deler av IKT-virksomheten knyttet opp mot foretakets øvrige mål. Foretaket skal ha dokumenterte prosedyrer for oppfølging av fastsatte kvalitetsmål.

§ 5 Sikkerhet

Foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, jf. § 1, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Kravene til IKT-sikkerhet skal så langt det er praktisk mulig være målbare. Oppfyllelse av kravene til informasjonssikkerhet for personopplysninger etter forskrift av 15.12.2000 nr 1265 til personopplysningsloven skal anses som oppfyllelse av kravene i paragrafen her.

§ 6 Utvikling og anskaffelse

Foretaket skal ha skriftlige prosedyrer for anskaffelse, utvikling, videreutvikling og testing av IKT-systemer. IKT-systemene skal ikke settes i ordinær drift før ansvarlig har godkjent dette.

§ 7 Systemvedlikehold

Foretaket skal sikre at IKT-systemene vedlikeholdes og forvaltes på en måte som gir en stabil, planlagt og forutsigbar drift. Det skal foreligge dokumenterte prosedyrer for systemvedlikeholdet.

§ 8 Drift

Driften av IKT-virksomheten skal være basert på dokumenterte prosedyrer, som sikrer fullstendig, rettidig og korrekt dataproduksjon, behandling og oppbevaring av produksjonsdata samt tilgjengelighet av IKT-systemene.

§ 9 Avviks- og endringshåndtering

Foretaket skal sikre at prosedyrer for avviks- og endringshåndtering foreligger og følges.

Prosedyrene for avvikshåndtering skal omfatte alle avvik som oppstår i driften av IKT-systemene. Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand i IKT-virksomheten. Avviksbehandlingen skal identifisere årsaken til avvik, hindre gjentagelser og sikre forsvarlig og formell behandling av avviket. Avvikene skal dokumenteres. Prosedyrene for avvikshåndtering skal inneholde retningslinjer for eskalering.

Prosedyrene for endringshåndtering skal omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av endringene. Foretaket skal sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift.

§ 10 Krav til kontinuitet

Foretaket skal ha en oppdatert kontinuitetsplan. Foretaket skal etablere en prosedyre for kontinuitet hvor roller, ansvarsoppgaver og risiko defineres. Foretaket skal med bakgrunn i risikoanalyse, jf. § 3, definere IKT-systemer av betydning for foretakets virksomhet som skal dekkes av kontinuitetsplanen. Kontinuitetsplanen skal blant annet inneholde:

- identifisering og vurdering av enkeltelementer som kan svikte og iverksette tiltak
- klare kriterier for oppstart av reserveløsningen
- gjenopprettingsprosedyrer
- informasjon til ledelse, ansatte, eventuelt kunder og leverandører

Det skal gjennomføres opplæring, øvelse og testing av reserveløsningene i et omfang som gir trygghet for at reserveløsningene fungerer tilfredsstillende. Testene skal dokumenteres slik at gjennomføring og resultat kan vurderes i ettertid.

§ 11 Driftsavbrudd og katastrofeberedskap

Foretaket skal ha en dokumentert katastrofeplan som skal iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en katastrofe. Med katastrofe menes hendelser som forårsaker driftsavbrudd slik at foretakets IKT-drift ikke kan fortsette med normalt tilgjengelige ressurser.

Katastrofeplanen skal minst omfatte:

- oversikt over IKT-systemer som inngår i katastrofeplanen
- beskrivelse av katastrofeløsningen
- klare kriterier for oppstart av katastrofeløsningen
- akseptabel lengde på et driftsavbrudd før katastrofeløsningen iverksettes
- prosedyrer som inneholder de nødvendige aktiviteter for å gjenopprette IKT-driften
- oversikt over ansvarsforhold og prosedyrer ved oppstart av katastrofeløsningen
- informasjon til berørte ansatte, leverandører, kunder, offentlige myndigheter og media

Det skal minst en gang årlig gjennomføres opplæring, øvelse og test i et omfang som gir tilstrekkelig trygghet for at katastrofeløsningen virker som forutsatt. Resultatet av testen skal dokumenteres slik at det er mulig å kontrollere.

§ 12 Utkontraktering

Foretaket har ansvar for at IKT-virksomheten oppfyller alle krav som stilles etter denne forskrift. Dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert. Det skal foreligge en skriftlig avtale som sikrer dette. Avtalen må sikre at foretak under tilsyn også gis rett til å inspisere og kontrollere de av leverandørens aktiviteter som er knyttet til avtalen. Avtalen skal også sikre håndtering av taushetsbelagt informasjon.

Avtalen skal videre sikre at Kredittilsynet gis tilgang til opplysninger fra og tilsyn hos IKT-leverandøren der Kredittilsynet finner det nødvendig som et ledd i tilsynet med foretaket.

Foretaket skal sikre, i egen regi eller gjennom et formalisert samarbeid med andre foretak enn IKT-leverandøren, at organisasjonen besitter tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalen.

§ 13 Dokumentasjon

Det skal foreligge en samlet oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten. Det skal foreligge oppdatert dokumentasjon av det enkelte IKT-system som er av betydning for foretakets virksomhet og som dokumenterer at forskriftens krav er oppfylt til enhver tid.

§ 14 Dispensasjon

Kredittilsynet kan gi dispensasjon fra forskriften eller deler av denne.

§ 15 Ikrafttredelse

Forskriften trer i kraft 1. august 2003. Samtidig oppheves forskrift av 16. desember 1992 nr. 1157 om bruk av informasjonsteknologi (IT). Kredittilsynet kan gi utsettelse med å oppfylle krav i forskriften.