Vegleiðing um eftirlits- og trygdartiltøk á KT-økinum sambært § 56, stk. 1, nr. 4, í løgtingslóg um tryggingarvirksemi

(Vejledning om kontrol- og sikringsforanstaltninger på it-området i henhold til løgtingslóg um tryggingarvirksemi § 56, stk. 1, nr. 4)

1. Indledning

Denne vejledning er udstedt i medfør af "løgtingslóg um tryggingarvirksemi" § 56, stk. 2, og omhandler Tryggingareftirlitið fortolkning af "løgtingslóg um tryggingarvirksemi" § 56, stk. 1, nr. 4, om betryggende kontrol- og sikringsforanstaltninger på it-området.

Vejledningen gælder for alle forsikringsselskaber, uanset størrelse.

2. Organisation

2.1 Bestyrelsen er ansvarlig for, og skal tage stilling til, virksomhedens it-anvendelse, herunder it-organisation og it-sikkerhed i form af f. eks. it-strategi, overordnet it-organisation og it-sikkerhedspolitik. I grundlaget for bestyrelsens stillingtagen skal indgå en vurdering af de risici, som virksomhedens it-anvendelse medfører.

2.2 Ansvaret for virksomhedens it-funktioner skal være klart defineret og placeret i organisationen.

2.3 Der skal være funktionsadskillelse mellem

- systemudvikling og -vedligeholdelse,
- it-drift samt
- virksomhedens forretningsførelse.

2.4 Idriftsætning af nye systemer, ændringer til eksisterende systemer og fejlrettelser skal ske under kontrollerede former.

3. It-sikkerhedspolitik

3.1 It-sikkerhedspolitikken fastsætter de overordnede krav til it-sikkerhedsniveauet i virksomheden. It-sikkerhedspolitikken skal i muligt omfang være uafhængig af den anvendte teknologi. Den skal revurderes periodisk, eksempelvis af hensyn til ændringer i virksomhedens forretnings- og it-mæssige risikoprofil samt ændringer i relevant lovgivning.

3.2 It-sikkerhedspolitikken kan, afhængig af virksomhedens størrelse, for eksempel omtale kravene til:

- Organisering af it-arbejdet, herunder funktionsadskillelse.
- Risikovurdering.
- Beskyttelse af systemer, data, maskinel og kommunikationsveje.
- Systemudvikling og vedligeholdelse af systemer.
- Driftsafvikling.
- Backup og sikkerhedskopiering.

- Genetablering af normal drift i tilfælde af fejl, nedbrud, tab af data eller systemer samt hel eller delvis ødelæggelse af bygninger, maskinel og kommunikationsveje.
- Kvalitetssikring
- Implementering af politikken i uddybende sikkerhedsbestemmelser, forretningsgange og instrukser.
- Forholdsregler i tilfælde af brud på it-sikkerhedspolitik og sikkerhedsregler.
- Overholdelse af relevant lovgivning.
- Rapportering, kontrol og opfølgning.
- Eventuelle dispensationer fra it-sikkerhedspolitikken.
- Outsourcing og kontrol hermed.

4. Forretningsgange

4.1 Der skal foreligge skriftlige forretningsgange, som klart beskriver forhold af væsentlig betydning for en betryggende håndtering af it-risici i virksomheden.

4.2 Forretningsgangene kan, afhængig af virksomhedens størrelse eller arten af it-anvendelsen, omfatte følgende:

- Efterlevelse af it-sikkerhedspolitik og bestemmelser.
- Placering af ansvar, herunder ejerskab for it-processer og -ressourcer.
- Overvågning af funktionsadskillelse.
- Kontrol med opretholdelse af det ønskede it-sikkerhedsniveau samt håndtering af eventuelle svagheder.
- Klassifikation og prioritering af systemer og data.
- Dokumentation af systemer (både basis- og brugersystemer) og ændringer.
- Sikkerhedskopiering af systemer og data, herunder opbevaring af sikkerhedskopierne.
- Anskaffelse af it-ressourcer.
- Systemudvikling, konfigurering og vedligeholdelse, samt afprøvning af nye og ændrede systemer.
- Test og anden kvalitetssikring.
- Ændringshåndtering og problemstyring.
- Adgangskontrol til systemer og data.
- Fysisk sikkerhed, herunder fysisk adgangskontrol.

5. Beredskabsplan

5.1 Der skal foreligge en it-beredskabsplan, hvis målsætning er godkendt af bestyrelsen. I planen kan, afhængig af virksomhedens forhold, beskrives etablering af beredskabsorganisation og aktivitetsplaner i tilfælde af alvorlige systemnedbrud, fejl og forstyrrelser i it-anvendelsen.

5.2 Der skal udarbejdes regler om afprøvning af beredskabsplan og rapportering af resultater af afprøvning.

6. Outsourcing

6.1 Ved outsourcing af it-funktioner skal virksomheden sikre sig, at leverandøren overholder dens it-sikkerhedspolitik og sikkerhedsregler. Der skal endvidere aftales procedurer, hvorefter virksomheden regelmæssigt kan kontrollere dette.

6.2 Outsourcing må ikke være til hindring for gennemførelse af virksomhedens beredskabsplan.

6.3 Outsourcing omfatter også tilfælde, hvor et eller flere selskaber i en koncern varetager drift, udvikling eller vedligeholdelse for andre selskaber i koncernen.

Tryggingareftirlitið, 15. desember 2008

Jógvan Thomsen

/ Katrina Maria Johannesen