INFORMATIONSSIKKERHEDSPOLITIK

Gyldig fra: 10. oktober 2014
Sidst opdateret: 22. Januar 2017

Introduktion

Dette dokument beskriver Worklife Barometers Informationssikkerhedspolitik, hvor dokumentet "Håndbog om Informationssikkerhedspolitik for Worklife Barometer" beskriver hvorledes sikkerhedspolitikken er implementeret.

Hensigten med sikkerhedspolitikken er at tilkendegive over for alle medarbejdere og eksterne samarbejdspartnere, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinjer. Det bemærkes i særdeleshed, at Worklife Barometers kerneprodukt Howdy er underlagt de strengeste krav fra Datatilsynet, da der foregår behandling af personfølsomme data.

Worklife Barometer ønsker derfor at opretholde og løbende udbygge et IT sikkerhedsniveau, der imødekommer enhver tid gældende lovgivning, samt specifikke forhold udstukket af Datatilsynet. For at sikre dette, entrerer Worklife Barometer med virksomhedens juridiske rådgiver, der pt. er Advokatfirmaet Bech-Bruun.

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at Worklife Barometer fremstår troværdig.

For at fastholde Worklife Barometers troværdighed skal det sikres, at information behandles med fornøden fortrolighed og at der sker fuldstændig, nøjagtig og rettidig behandling af godkendte transaktioner.

IT-systemer betragtes som Worklife Barometers mest kritiske ressource. Der lægges derfor vægt på drift, sikkerhed, kvalitet, overholdelse af lovgivningskrav og på at systemerne er brugervenlige, dvs. uden unødigt besværlige sikkerheds-foranstaltninger.

Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, således at Worklife Barometers image og medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Beskyttelsen skal være vendt imod såvel naturgivne som tekniske og menneskeskabte trusler. Alle personer betragtes som værende mulig årsag til brud på sikkerheden; dvs. at ingen persongruppe skal være hævet over sikkerhedsbestemmelserne.

Målene er derfor, at:

- opnå høj driftssikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og datatab
  dvs. **TILGÆNGELIGHED**
- opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl i såvel data som systemer
  dvs. **INTEGRITET**
- opnå fortrolig behandling, transmission og opbevaring af data
  dvs. **FORTROLIGHED**
- opnå en gensidig sikkerhed omkring de involverede parter
  dvs. **AUTENTICITET**
- opnå en sikkerhed for gensidig og dokumenterbar kontakt
  dvs. **UAFVISELIGHED**

Alle Worklife Barometers medarbejder er gjort eksplicit opmærksomme på Worklife Barometers Informationssikkerhedspolitik og alle Databehandlere (der ikke databehandler IT Services) til Worklife

Barometer er oplyst om virksomhedens Informationssikkerhedspolitik gennem Databehandleraftaler og Service Level Agreements (SLAs) (hvor nødvendigt).

Regler og retningslinjer fra informationssikkerhedspolitikken bliver løbende indarbejdet i de relevante gældende regler på personalepolitikkens område.

Omfang

Sikkerhedskonceptet omfatter følgende:

- En informationssikkerhedspolitik, der godkendes af direktionen på baggrund af indstilling fra Udvalget for informationssikkerhed.
- Sikkerhedsinstrukser og –procedurer, som formuleres af respektive forretningsområdeejere ud fra krav og retningslinjer beskrevet "Håndbog om Informationssikkerhedspolitik for Worklife Barometer"

Gyldighedsområde

Politikken er gældende for alle Worklife Barometers informationsrelaterede aktiviteter, uanset om disse udføres af ansatte i Worklife Barometer eller af Databehandlere til Worklife Barometer.

Organisation og ansvar

Det delegerede sikkerhedsrelaterede ansvar og den tilhørende myndighed er generisk beskrevet/rollefordelt i "Håndbog om Informationssikkerhedspolitik for Worklife Barometer" til denne politik.

Beredskabsplanlægning

Katastrofer søges undgået gennem en veltilrettelagt overvågning af de til en hver tid benyttede IT services. Omfanget af disse foranstaltninger besluttes ud fra en afvejning af risici i mod sikringsomkostninger og brugervenlighed.

Worklife Barometers beredskabsplan indeholder følgende områder:

- Skadebegrænsende tiltag
- Etablering af temporære nødløsninger
- Genetablering af permanent løsning

Beredskabsplanerne skal ajourføres og testes løbende – og minimum en gang om året.

Sanktionering

Medarbejdere, der bryder de gældende informationssikkerhedsbestemmelser i Worklife Barometer, kan straffes disciplinært. De nærmere regler om dette fastsættes i overensstemmelse med den gældende personalepolitik.