# Informationssikkerhedspolitik for <Virksomhedsnavn>

## 1 Målsætning/formål

Sikkerhedspolitikken skal til enhver tid understøtte <virksomhedsnavn>s værdigrundlag og vision samt de strategiske mål, der er i IT-strategien.

Hensigten med sikkerhedspolitikken er endvidere at tilkendegive over for alle, som har en relation til <virksomhedsnavn>, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinier.

<Virksomhedsnavn> ønsker derfor at opretholde og løbende udbygge et IT sikkerhedsniveau på højde med de krav, som skitseres i 'Den fællesstatslige standard for informationssikkerhed' (DS 484 basale krav). Kravene skærpes på veldefinerede områder, hvor der er specielle lovkrav, aftaleretslige forhold eller evt. særlig risiko (afdækket ved en risikovurdering).

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at <virksomhedsnavn> fremstår troværdig både nationalt og internationalt.

For at fastholde <virksomhedsnavn>s 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, næst efter medarbejderne, som <virksomhedsnavn>s mest kritiske ressource. Der lægges derfor vægt på driftsikkerhed, kvalitet, overholdelse af lovgivningskrav og på at systemerne er brugervenlige, dvs. uden unødigt besværlige sikkerhedsforanstaltninger.

Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, således at <virksomhedsnavn>s 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 driftsikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og datatab - TILGÆNGELIGHED
- opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl i såvel data som systemer - INTEGRITET
- opnå fortrolig behandling, transmission og opbevaring af data - FORTROLIGHED
- opnå en gensidig sikkerhed omkring de involverede parter - AUTENTICITET
- opnå en sikkerhed for gensidig og dokumenterbar kontakt - UAFVISELIGHED

Ovenstående mål skal konkretiseres i Service Level Agreements (SLAs) og kontrakter overfor samarbejdspartnere.

Regler og retningslinjer fra informationssikkerhedspolitikken skal løbende indarbejdes i de relevante gældende regler på personalepolitikkens område.

## 2. Omfang

Sikkerhedskonceptet omfatter følgende:

- En informationssikkerhedspolitik, der godkendes af direktionen på baggrund af indstilling fra Udvalget for informationssikkerhed.
- En informationssikkerhedshåndbog, der uddyber informationssikkerhedspolitikken, fastlægges af Udvalget for informationssikkerhed.
- Sikkerhedsinstrukser og –procedurer, som formuleres af respektive ejere og liniechefer ud fra krav og retningslinier i informationssikkerhedshåndbogen
- En 12-trins styringsmodel opbygget efter Plan, Do, Check, Act principperne i BS 7799 Del 2 : 2002 og anbefalet af det fællesstatslige sikkerhedsprojekt.

### 3. Gyldighedsområde

Politikken er gældende for alle <virksomhedsnavn>s informationsrelaterede aktiviteter, uanset om disse udføres af ansatte i <virksomheden> eller af samarbejdspartnere. Dette inkluderer f.eks. alle data om personale, data om finasielle forhold, alle data som bidrager til administrationen af virksomheden, produktionsdata og anlægsdata samt informationer som er overladt til <virksomhedsnavn> af andre. Disse data kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning eller anden information, som kun er til intern brug.

Informationssikkerhedspolitikken har gyldighed for alle ansatte i <virksomhedsnavn> og al anvendelse af <virksomhedsnavn>s informationsaktiver.

### 4. Organisation og ansvar

Det delegerede sikkerhedsrelaterede ansvar og den tilhørende myndighed er generisk beskrevet/rollefordelt i Bilag 1 til denne politik.

### 5. Beredskabsplanlægning

Katastrofer søges undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og IT-udstyr. Omfanget af disse foranstaltninger besluttes ud fra en afvejning af risici i mod sikringsomkostninger og udmøntes i SLAs.

<Virksomhedsnavn>s beredskabsplan aftales med KIT og indarbejdes i dennes overordnede beredskabsplan. Heri skal hhv. <virksomhedsnavn>s og partnernes ansvar for sikkerhedskopiering og nødplaner entydigt præciseres.

Beredskabsplanerne skal omfatte:

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

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

### 6. Sanktionering

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

## Bilag 1 Organisation og ansvar

### 1. Udvalget for informationssikkerhed

Udvalget består af:

- Administrationschefen (formand for udvalget)
- <Virksomheden>'s IT-sikkerhedskoordinator (sekretær for udvalget),

samt repræsentanter fra relevante aktører/interessenter i <virksomhedsnavn>

- Kontorchefen for ***
- En repræsentant for *** på ledelsesniveau
- En – eller flere – repræsentanter for brugerfunktionerne

Udvalget er normgivende og fastsætter på grundlag af den vedtagne informationssikkerhedspolitik de principper/retningslinier, der skal sikre målopfyldelsen.

Udvalget behandler alle sikkerhedsspørgsmål af principiel karakter.

Udvalget foretager en årlig vurdering af informationssikkerhedspolitikken og de tilknyttede sikkerhedsretningslinier – herunder at disse lever op til de eksterne forpligtelser udtrykt i lovgivning og kontrakter/aftaler. Udvalget vurderer samtidigt, om der er behov for fornyet risikovurdering/ konsekvensanalyse.

Udvalget kan ad hoc lade sig supplere med faglig assistance fra IT-Sikkerhedsfunktionen

Ansvaret behandles i øvrigt i sikkerhedshåndbogens afsnit 6.1.2 (også DS 484:2005 reference)

*** den interne IT-sikkerhedsfunktion.

## 2. IT Sikkerhedsfunktionen

*Formuleres efter situationen*
På grund af <virksomhedsnavn>s store grad af outsourcing af drift og support til Koncern-IT og derigennem ofte til større, professionelle samarbejdspartnere er det ikke hensigtsmæssigt at operere med en større særskilt/funktionsadskilt IT Sikkerhedsafdeling/-funktion. I stedet løses opgaverne primært ved:

- at tage hensyn hertil i aftalegrundlag med samarbejdspartnere, f.eks. ved at pålægge samarbejdspartnere at foretage forskellige former for kontrol og opfølgning og rapportere herom til Udvalget for informationssikkerhed
- at iværksætte egne revisionsopgaver og/eller sikkerhedsundersøgelser i det omfang Udvalget for informationssikkerhed finder det fornødent.

Funktionen har ansvar for:

- At udarbejde og vedligeholde sikkerhedshåndbogen indeholdende sikkerhedsprincipper for informations anvendelsen – evt. med ekstern assistance
- At udarbejde relevante sikkerhedskrav, der operationaliserer informationssikkerhedspolitikken – evt. med ekstern assistance
- At foretage opfølgning og rapportering af sikkerhedsbrud til Udvalget for informationssikkerhed – evt. outsourcet, hvor dette kan ske betryggende
- At behandle dispensationsansøgninger for begrundede afvigelser i forhold til retningslinierne og rapportere disse til Udvalget for informationssikkerhed
- At holde sig ajour med den generelle udvikling på det sikkerhedsmæssige område
- At koordinere relevante initiativer med de øvrige aktører i koncernsamarbejdet

Ansvaret behandles i øvrigt i sikkerhedshåndbogens afsnit 6.1.2 (også DS 484:2005 reference)

## 3. Linieledelsen

Den enkelte chef i linien – herunder direktionen - har ansvar for:

- At informationssikkerhedspolitikken og de regler, der er relevante for hans/hendes ansvarsområde, er kendte og efterleves
- At medarbejderne gennem uddannelse og udvikling opnår sikkerhedsbevidsthed om nødvendigheden af at overholde de sikkerhedsmæssige retningslinjer og at disse efterleves
- At der, efter behov, udarbejdes yderligere dokumentation vedr. sikkerhed for <virksomheden>s/kontorets område
- At der ved installation af nye systemer gennemføres en forudgående sikkerheds-/risikovurdering
- At koordinere opklaringsarbejdet ved konstateret eller begrundet mistanke om sikkerhedsbrud. Resultatet rapporteres til IT Sikkerhedsfunktionen
- At retningslinierne for ansættelse, introduktion, løbende vurdering, funktionsskift og afvikling af medarbejdere overholdes

Der skal tilstræbes uafhængighed af enkeltpersoner gennem etablering af personbackup for de medarbejdere, der er alene om at dække specialer eller systemer af væsentlig betydning for <virksomhedsnavn>. Som supplement hertil skal dokumentationen tilhørende disse områder også holdes ajourført og evt. udbygges.

Ansvaret behandles i øvrigt i sikkerhedshåndbogens afsnit 6.1.1 (også DS 484:2005 reference)

## 4. Systemejere

System ejere har ansvar for:

- at der udarbejdes en kravspecifikation som tager eksplicit hensyn til sikkerhedsmæssige forhold forud for enhver systemudvikling/ –ændring/-anskaffelse /-opdatering – evt. med ekstern assistance
- at der udarbejdes en risikovurdering i h.t. kravene hertil
- at Change Management retningslinierne følges ved enhver ændring af systemet
- at der ved idriftsætning af systemet foreligger konkrete regler og procedurer for regulering og administration af adgangsforholdene – og at disse er i overensstemmelse med de principielle krav hertil
- at autorisere adgangen til systemet i h.t. retningslinierne herfor
- at foretage opfølgning og rapportering af sikkerhedsbrud til Udvalget for informationssikkerhed – evt. outsourcet, hvor dette kan ske betryggende

I de situationer, hvor der ikke er funktionsadskillelse (autorisation/ administration) kompenseres med andre sikkerhedsforanstaltninger, som udmøntes i retningslinierne og konkret i regler og procedurer for systemadministrationen.

## 5. Dataejere

Dataejeren har ansvar for:

- at der udarbejdes en risikovurdering i h.t. kravene hertil – for systemtilknyttede data i samarbejde med systemejeren
- at der inden indrapportering af data i systemer foreligger konkrete regler og procedurer for regulering og administration af adgangsforholdene – og at disse er i overensstemmelse med de principielle krav hertil

- at autorisere adgangen til data i h.t. retningslinierne herfor samt at sikre, at enhver sikkerhedsmæssig følsom informationsaktivitet kan henføres til den person, som har udført aktivteten
- at foretage opfølgning og rapportering af sikkerhedsbrud til Udvalget for informationssikkerhed

I de situationer, hvor der ikke er funktionsadskillelse (autorisation/ administration) kompenseres med andre sikkerhedsforanstaltninger, som udmøntes i retningslinierne og konkret i regler og procedurer for dataadministrationen.

## 6 Ejere af fysiske aktivier

Alle fysiske aktiver får udpeget/ tildelt en ejer.
Såfremt aktivet er omfattet af en aftale om hosting, tages der hensyn hertil i aftalegrundlaget med samarbejdspartneren, f.eks. ved at pålægge samarbejdspartneren at foretage forskellige former for kontrol og opfølgning og rapportere herom.

Ejeren af det fysiske aktiv har ansvar for:
- at der udarbejdes en kravspecifikation ved placering, indretning, forandring m.v. som tager eksplicit hensyn til sikkerhedsmæssige forhold – evt. med ekstern assistance
- at der udarbejdes en risikovurdering i h.t. kravene hertil
- at der ved ibrugtagning af lokaler/udstyr foreligger konkrete regler og procedurer for regulering og administration af adgangsforholdene – og at disse er i overensstemmelse med de principielle krav hertil
- at autorisere adgangen til lokalerne/ udstyret i h.t. retningslinierne herfor
- at foretage opfølgning og rapportering af sikkerhedsbrud til Udvalget for informationssikkerhed – evt. outsourcet, hvor dette kan ske betryggende

I de situationer, hvor der ikke er funktionsadskillelse (autorisation/ administration) kompenseres med andre sikkerhedsforanstaltninger, som udmøntes i retningslinierne og konkret i regler og procedurer for fysisk sikkerhed og adgangsadministrationen.

## 7. Medarbejdere

Funktionsadskillelse er det bærende kontrolprincip såvel på person- som på organisationsplanet. Hvor dette ikke er praktisk eller økonomisk hensigtsmæssigt, skal kompenserende kontroller indføres.

Den enkelte medarbejder har ansvar for:
- At overholde informationssikkerhedspolitikken og de regler, der er relevante for den enkeltes arbejdsopgaver
- At rapportere om eventuelle sikkerhedsbrud eller mistanke herom til nærmeste chef og til IT-Sikkerhedsfunktionen

## 8. Samarbejdspartnere

Samarbejdspartnere – herunder KIT - bærer p.g.a. det valgte koncept en meget væsentlig del af ansvaret for at det valgte sikkerhedsniveau etableres og opretholdes.
Samarbejdspartnerne har ansvar for:

- At <virksomhedsnavn>s informationssikkerhedspolitik og de regler, der er relevante for deres ansvarsområde, er kendte og efterleves – mest hensigtsmæssigt ved at egne sikkerhedspolitikker og regler til enhver tid afspejler krav fra < virksomhedsnavn >
- At medarbejderne gennem uddannelse og udvikling opnår sikkerhedsbevidsthed om nødvendigheden af at overholde de sikkerhedsmæssige retningslinjer, herunder tiltrædelseserklæringen
- At der, efter behov, udarbejdes yderligere dokumentation vedr. sikkerhed for samarbejdspartnerens område
- At der ved installation af nye og modifikation af eksisterende interne systemer og komponenter med påvirkningsmulighed til <virksomhedsnavn>s informationsaktiver gennemføres en forudgående risiko-/sikkerhedsvurdering
- At koordinere opklaringsarbejdet ved konstateret eller begrundet mistanke om sikkerhedsbrud. Hændelsen og resultatet rapporteres via egen sikkerhedsorganisation til <virksomhedsnavn>s IT Sikkerhedsfunktion

## IT-Sikkerhedsregler/håndbog -

Indholdsfortegnelse for <virksomhedsnavn>s IT-sikkerhedshåndbog

Dette er en oversigt over punkter i IT-sikkerhedshåndbogen, udarbejdet af Dansk Standard. For nærmere uddybelse af samtlige underpunkter, se 'Forøg virksomhedens informationssikkerhed', et hæfte udarbejdet gennem et samarbejde mellem Dansk Standard Center for ICT, ITEK og Dansk Industri.
Hæftet kan erhverves i Dansk Industri's butik på www.di.dk

***DS 484:2005 struktur***.
**Indholdsfortegnelse**
Indledning
IT sikkerhedsorganisation i <virksomhedsnavn>