Delpolitik for Informationssikkerhed - 2017

Indledning
Nærværende politik, der er baseret på retningslinjerne i standarden for informationssikkerhed: ISO 27001, udgør de overordnede rammer for arbejdet med informationssikkerheden på DTU. Det medfører, at de efterfølgende retningslinjer, regler og forretningsgange skal være detaljerede og et konkret udtryk for denne politik.

På baggrund af en indstilling fra IT-Sikkerhedsforum tager direktionen Informationssikkerhedspolitikken op til revurdering hvert andet år.

Udgangspunktet for informationssikkerhedsarbejdet er en risikovurdering, der gennemføres på alle enheder, der refererer til DTU's direktion. Risikovurderingen tager afsæt i de fire hovedforretnings-områder på DTU; uddannelse, forskning, forskningsbaseret rådgivning og innovation.

Formål
Den viden, DTU har akkumuleret igennem tiden, samt den viden, der i dag bliver udviklet på DTU, er en vigtig del af virksomhedens fundament. Informationssikkerheden har derfor vital betydning for DTU's troværdighed og funktionsdygtighed.
Formålet med politikken er at definere rammerne for beskyttelse af DTU's informationer – herunder at fastlægge fordelingen af ansvar og opgaver. I særdeleshed skal politikken sikre, at kritiske og følsomme informationer og informationssystemer bevarer deres fortrolighed, integritet og tilgængelighed.

Omfang
Politikken omfatter information der tilhører DTU, samt informationer der er i DTU's varetægt. DTU er her defineret som værende de enheder, der refererer til DTU's Direktion.

Politikken gælder ansatte, studerende og personer med midlertidig tilknytning til DTU.

Ved udlicitering af opgaver eller drift skal det sikres i aftalen med leverandøren, at DTU's sikkerheds-niveau fastholdes.

Sikkerhedsniveau
Det er DTU's politik at beskytte sine informationer samt informationer overladt i DTU's varetægt, og udelukkende tillade brug, adgang og offentliggørelse af informationer i overensstemmelse med informationssikkerhedspolitikkens overordnede retningslinjer og under hensyntagen til den til enhver tid gældende lovgivning.

DTU tilstræber et informationssikkerhedsniveau, der afspejler konkrete risikovurderinger udført af de forretningsansvarlige for det pågældende område. Direktionen har fastlagt de basale sikringsforanstaltninger, og dette er beskrevet i de til enhver tid gældende retningslinjer, regler, procedurer og forretningsgange. Ligeledes har DTU's direktion besluttet, at hensynet til informationssikkerhed skal integreres i alle forretningsgange, driftsopgaver og projekter.

Samtidig skal IT-sikkerhedssystemet tilpasses, så DTU kan fungere med en høj grad af åbenhed overfor studerende, der færdes på Campus og i forhold til en række tætte samarbejdsrelationer til forskere fra hele verden og til eksterne virksomheder. Det fordrer på den ene side systemer, der er åbne for en bred

kreds af brugere - men også muligheden for at beskytte udvalgte data og systemer ekstra meget. Så vidt det er muligt indenfor rammerne og ikke påvirker sikkerheden, skal brugervenlighed altid prioriteres.

IT-systemerne skal endvidere respektere og understøtte ønsket om højere grad af mobilitet i arbejdsstyrken. Det indebærer skiftende krav pga. diffus geografisk afgrænsning samt håndteringen af adgangen til DTU's systemer fra mange forskellige datamedier (Smartphones, Tablets mv.).

Sikkerhedsbevidsthed
Alle ansatte, studerende og personer med midlertidig tilknytning til DTU har et ansvar for at bidrage til at beskytte DTU's informationer mod uautoriseret adgang, ændring, ødelæggelse og tyveri. Alle ansatte, studerende og personer med midlertidig tilknytning skal derfor løbende informeres om informationssikkerhed i relevant omfang.

Såfremt en trussel mod informationssikkerheden eller brud på denne opdages, skal dette straks meddeles til den IT-sikkerhedsansvarlige.

Personer som bryder informationssikkerhedspolitikken eller deraf afledte regler, kan blive udsat for disciplinære forholdsregler i overensstemmelse med DTU's gældende regler og politikker.

Organisering
Det overordnede ansvar for Informationssikkerhed ligger hos DTU's ledelse. Der er nedsat et centralt Informationssikkerhedsudvalg med en repræsentant for DTU's ledelse som formand. Dette udvalg har ansvaret for, at målsætninger indenfor informationssikkerhed nås, og at der løbende opnås forbedringer.

Ansvaret for og opgaven med informationssikkerhed i enhederne er placeret hos enhedernes ledelser. Dette skal fremgå af enhederne's UMV og handleplaner.
Det operationelle ansvar for den daglige styring af informationssikkerhedsindsatsen, er placeret hos IT-sikkerhedskoordinatoren, der refererer til Underdirektøren for IT. Koordinatoren skal sikre, at de tiltag, der er beskrevet i informationssikkerhedspolitikkens tilknyttede dokumenter, gennemføres og efterleves. Derudover påhviler det IT-Sikkerhedskoordinatoren at sikre vidensdeling mellem enhederne og at medvirke til etableringen af fælles tiltag indenfor Informationssikkerhed. Til denne opgave er etableret IT-Sikkerhedsforum, hvor den IT-Sikkerhedsansvarlige fra alle enheder er medlem, samt IT-Sikkerhed-Teknik, hvor den IT-ansvarlige fra alle enheder er medlem.

De styrende dokumenter er som følger:
1. Delpolitik for Informationssikkerhed (dette dokument)
2. Overordnede retningslinjer
3. Fælles regler for informationssikkerhed (2016)

DTU, december 2016
Udarbejdet af DTU's IT-sikkerhedsforum
Godkendt af DTU's direktion