IT-sikkerhedsramme for EnergyDataDK (ISO27001)

Introduktion

PowerLabDK/EnergyDataDK har lagt DTU's IT-sikkerhedspolitikker og DTU Vind og Energisystemer's retningslinjer til grundlag for sit arbejde med informationssikkerhed. DTU's overordnede IT-sikkerhedspolitikker anvender ISO standard ISO27001 som grundlag og IT-sikkerhedsarbejdet for EnergyDataDK afspejler derfor også dette.

DTU Security Operation fastlægger de overordnede mål med IT Sikkerhedsarbejdet, definerer en række formelle roller og deres ansvarsområder, begreber samt fastlægger en klassifikationsskala mv, mens DTU's institutter har en implementerende samt vejledende rolle.

Emnespecifikke IT-sikkerhedspolitikker

DTU har besluttet at implementere sikringstiltag, der indgår i ISO27001 annex A med tilhørende uddybning i ISO-standard 27002, gennem en række emnespecifikke IT-sikkerhedspolitikker og har formuleret en række krav, der skal opfyldes for at sikre at DTU's informationssikkerhedspolitik overholdes.

For EnergyDataDK er der udpeget en række emnespecifikker politiker, som er vurderet relevante for efterlevelsen. Der drejer sig om:

- Klassificering og styring
- Identitet og adgangsstyring
- Systemdrift
- Logning
- Sikkerhedskopiering ("Backup & Restore")
- Software vedligehold ("Patch Management")
- Fortsat drift

Reference til ISO27002 foranstaltninger

De krav, der følger af de udpegede emnespecifikke politikker, omfatter samlet set følgende ISO 27002-foranstaltninger for EnergyDataDK:

Klassificering og styring:

5.8: Informationssikkerhed i projekter
5.9: Fortegnelse over information og understøttende aktiver
5.10: Acceptabel brug af information og understøttende aktiver
5.13: Mærkning af information
5.14: Overførsel af information
6.3: Awareness, uddannelse og træning vedrørende informationssikkerhed
8.12: Forebyggelse af datalækage

Identitet og adgangsstyring:

- 5.3: Funktionsadskillelse
- 5.11: Returnering af aktiver
- 5.15: Administration af adgang
- 5.16: Styring af identifikation
- 5.17: Autentifikationsoplysninger
- 5.18: Adgangsrettigheder
- 6.5: Ansvar i forbindelse med ophør eller ændring af ansættelsesforhold
- 8.2: Privilegerede adgangsrettigheder
- 8.3: Begrænset adgang til information
- 8.5: Sikker autentifikation
- 8.18: Brug af privilegerede understøttende programmer

Systemdrift

- 5.37: Dokumenterede driftsprocedurer
- 8.6: Kapacitetsstyring
- 8.9: Konfigurationsstyring
- 8.10: Sletning af information
- 8.17: Synkronisering af ure
- 8.18: Brug af privilegerede understøttende programmer
- 8.31: Adskillelse af udviklings-, test- og produktionsmiljøer
- 8.32: Ændringsstyring
- 8.34: Beskyttelse af informationssystemer under audit

Logning

- 8.15: Logning
- 8.16: Overvågning af aktiviteter

Sikkerhedskopiering (”Backup & Restore”)

- 8.13: Backup af information

Software vedligehold (”Patch Management”)

- 8.8: Styring af tekniske sårbarheder

Fortsat drift

- 5.29: Informationssikkerhed under driftsforstyrrelse
- 5.30: IKT-parathed til understøttelse af business continuity
- 7.11: Forsyningssikkerhed
- 8.6: Kapacitetsstyring
- 8.14: Redundans i faciliteter til informationsbehandling

Ansvar, efterlevelse, kontrol og auditering

Efterlevelse af de emnespecifikke IT-sikkerhedspolitikker er først og fremmest et ansvar for indehaveren af informationsaktivet/systemet. Dokumenter, der udarbejdes i forbindelse med

efterlevelsesvurderingen af EnergyDataDK, dokumenterer, hvordan de relevante emnespecifikke IT-sikkerhedspolitikker er implementeret.

For EnergyDataDK er der desuden tre procedurebeskrivelser, som i praksis beskriver, hvordan de relevante politikker er implementeret. Det drejer sig om:

1. Backup and restore procedure
2. Identity and Access Management
3. Operation and maintenance

DTU anvender ISMS-systemet 'Control Manager' til at styre og dokumentere ajourføringen af politikker, procedurebeskrivelser og periodiske kontroller. EnergyDataDK er registreret som system hos DTU Vind og Energisystemer og indgår dermed i denne fælles styringsproces.

Intern kontrol, auditering og den overordnede efterlevelse af DTU's IT-sikkerhedspolitik indgår desuden i DTU's overordnede processer for risiko- og sårbarhedsvurdering.

GDPR, NIS 2 samt øvrige DTU-politikker og retningslinjer

Ved udarbejdelsen af DTU's IT-sikkerhedspolitik er en række relevante aktører på DTU blevet inddraget. Formålet har været at sikre, at politikken så vidt muligt også adresserer krav og behov i DTU's øvrige politikker og retningslinjer, herunder persondatapolitik (GDPR) og NIS 2.

DTU baserer for nuværende sin implementering af NIS 2-direktivet på nævnte DTU IT-sikkerhedspolitik og det tilhørende ledelsessystem for informationssikkerhed (ISMS).

DTU's IT-sikkerhedspolitik udgør dog ikke en garanti for, at øvrige DTU-politikker efterleves og EnergyDataDK arbejder derfor særskilt med efterlevelsen af øvrige politikker inkl. lovmæssige krav, herunder GDPR og Dataforordningen.