IT security framework for EnergyDataDK (ISO27001)

Introduction

PowerLabDK/EnergyDataDK has used DTU's IT security policies and DTU Wind and Energy Systems' guidelines as the basis for its work with information security. DTU's overall IT security policies use ISO standard ISO27001 as a basis, and the IT security work for EnergyDataDK therefore also reflects this.

DTU Security Operation establishes the overall goals of IT Security Work, defines several formal roles and their areas of responsibility, concepts, and establishes a classification scale, etc., while DTU's departments have an implementing and guiding role.

Subject-specific IT security policies

DTU has decided to implement security measures included in ISO27001 Annex A with associated elaboration in ISO standard 27002 through several subject-specific IT security policies and has formulated several requirements that must be met to ensure that DTU's information security policy is complied with.

For EnergyDataDK, several topic-specific policies have been identified that are deemed relevant for compliance. These include:

- Classification and management
- Identity and access management
- System operation
- Logging
- Backup & Restore
- Software maintenance ("Patch Management")
- Continued operation

Reference to ISO27002 measures

The requirements resulting from the designated topic-specific policies collectively include the following ISO 27002 measures for EnergyDataDK:

Classification and management:

5.8: Information security in projects
5.9: Inventory of information and supporting assets
5.10: Acceptable Use of Information and Supporting Assets
5.13: Labelling of information
5.14: Transfer of information
6.3: Awareness, education and training regarding information security
8.12: Preventing Data Leakage

Identity and access management:

- 5.3: Separation of functions
- 5.11: Return of assets
- 5.15: Managing Access
- 5.16: Management of identification
- 5.17: Authentication information
- 5.18: Access rights
- 6.5: Liability in connection with termination or change of employment
- 8.2: Privileged access rights
- 8.3: Limited access to information
- 8.5: Secure authentication
- 8.18: Use of privileged supporting applications

System operation

- 5.37: Documented operating procedures
- 8.6: Capacity management
- 8.9: Configuration Management
- 8.10: Deletion of information
- 8.17: Synchronizing Clocks
- 8.18: Use of privileged supporting applications
- 8.31: Separation of development, test and production environments
- 8.32: Change management
- 8.34: Protection of information systems under audit

Logging

- 8.15: Logging
- 8.16: Monitoring of activities

Backup & Restore

- 8.13: Backup of information

Software maintenance ("Patch Management")

- 8.8: Management of technical vulnerabilities

Continued operation

- 5.29: Information security during operational disruption
- 5.30: ICT readiness to support business continuity
- 7.11: Security of supply
- 8.6: Capacity management
- 8.14: Redundancy in information processing facilities

Accountability, Compliance, Control and Auditing

Compliance with the topic-specific IT security policies is first and foremost a responsibility for the owner of the information asset/system. Documents prepared in connection with the compliance

assessment of EnergyDataDK document how the relevant topic-specific IT security policies are implemented.

For EnergyDataDK, there are also three procedure descriptions, which in practice describe how the relevant policies are implemented. These are:

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

DTU uses the ISMS system 'Control Manager' to manage and document the updating of policies, procedure descriptions, and periodic controls. EnergyDataDK is registered as a system with DTU Wind and Energy Systems and is thus part of this joint management process.

Internal control, auditing, and overall compliance with DTU's IT security policy are also part of DTU's overall processes for risk and vulnerability assessment.

GDPR, NIS 2 and other DTU policies and guidelines

In the preparation of DTU's IT security policy, several relevant actors at DTU have been involved. The purpose has been to ensure that the policy also addresses the requirements and needs of DTU's other policies and guidelines, including the General Data Protection Policy (GDPR) and NIS 2.

DTU currently bases its implementation of the NIS 2 directive on the above-mentioned DTU IT security policy and the associated information security management system (ISMS).

However, DTU's IT security policy does not constitute a guarantee that other DTU policies are complied with, and EnergyDataDK therefore works separately with compliance with other policies, including legal requirements, including GDPR and the Data Protection Regulation.