Klima-, Energi- og Forsyningsministeriet

One-pager on critical infrastructure and cybersecurity in the offshore wind industry

Developers and operators of offshore wind turbines must at all times comply the existing rules e.g. on emergency preparedness and cybersecurity. On 7 March 2025, the Act on Strengthened Preparedness in the Energy Sector entered into force, implementing, among other things, the EU's NIS2 and CER Directives in the energy sector. The purpose of the Act is to enhance resilience and emergency preparedness against natural, man-made and technological threats to Danish energy supply across all energy sources.

Among other things, the Act entails that developers and operators must comply with a number of cyber and physical security requirements, including protection against insecure or unauthorized remote access.

Requirements for supplier management and risk and vulnerability management under the Act on Strengthened Preparedness in the Energy Sector

According to the Executive Order on Resilience and Emergency Preparedness in the Energy Sector issued under the Act on Strengthened Preparedness in the Energy Sector, entities covered by the regulation must, among other things.:

- Be able to identify, assess and manage risks specific to each direct supplier and service provider in the company's supply chain, and have methods for assessing the resilience of the supplied products.
- Address risks associated with dependencies on subcontractors and international conditions in agreements with direct suppliers and service providers.
- Have procedures for managing remote access for direct suppliers and service providers who may access the company's supply-critical network and information systems.
- Ensure that requirements concerning organisational preparedness, physical security and cybersecurity are included in the company's supplier agreements with direct suppliers or service providers.
- Conduct risk assessments for the following projects: (1) acquisition and development of supply-critical network and information systems, (2) establishment of new installations or acquisition of installations with class 3–5, (3) modification of existing installations with class 3–5 that are expected to change an installation's classification, and (4) outsourcing of development, operation and maintenance tasks that may affect the delivery of the company's services.
- Ensure compliance with requirements concerning organisational preparedness, physical security and cybersecurity.
- Ensure that any project involving a supplier relationship includes a risk assessment of risks arising from that supplier relationship. The risk assessment must be prepared at the start of the project and be available in written form before the project commences. The risk assessment must be updated when the project's scope, timeline or deliverables change to an extent that alters the assumptions underlying the assessment.
- Submit risk assessments to the Danish Energy Agency for approval in connection with the following projects: (1) installation projects in which the completed installation is expected to meet the threshold values for class 4 or 5 installations, and (2) acquisition or development of supply-critical network and information systems.
- Submit risk assessments to the Danish Energy Agency no later than one month after their approval by the company's management body.
- Companies in levels 4 and 5 must place servers and data centers supporting their supply-critical network and information systems within EU/EEA countries.

Kilde: The Danish Ministry of Climate, Energy and Utilities.