Danish Energy Agency

Executive Order on resilience and preparedness in the energy sector
No 260 of 25 March 2025

Unofficial translation of "Bekendtgørelse om modstandsdygtighed og beredskab i energisektoren"

Pursuant to Section 4(3), Section 5(3 & 4), Section 6(2), Section 7(2), Section 8(2), Section 8(2), Section 10, Section 12, Section 13, Section 19(4 & 5), Section 22(3), Section 23(4), Section 26(2), Section 30, Section 32(1), Section 34, Section 35(2), Section 36 and Section 37(4) of Act no. 258 of 6 March 2025 on enhanced preparedness in the energy sector and after consultation with the Minister for Resilience and Preparedness, by authorisation it is hereby established pursuant to Section 4, sub-section 1, no. 34 and sub-section 2 and Section 5 of Executive Order No. 259 of 6 March 2025 on the tasks and powers of the Danish Energy Agency that:

Chapter 1
Purpose, scope and definitions

Section 1. This Executive Order sets out rules on organisational preparedness, physical security and cybersecurity for operations that are essential for the energy supply and energy markets in Denmark and Europe. The Executive Order also lays down rules for the Danish Energy Agency and the Energinet's tasks in connection with preparedness in the energy sector.

Section 2. The Executive Order applies to enterprises covered by Section 2 of the Act on Enhanced Preparedness in the Energy Sector, however, cf. Section 5.

(2) The rules on measures to support the resilience of plants pursuant to Chapter 10 shall apply to enterprises with installations classified under Section 6(2), however, cf. Sections 8, 42 and 43.

(3) The rules on measures to support the security of networks and information systems set out in this Executive Order shall apply to the networks and information systems used by enterprises for their operations or for the provision of their services, cf. Section 8 of the Act on Enhanced Preparedness in the Energy Sector.

Section 3. For the purposes of this Executive Order, the following terms are to be understood as :

1) Preparedness: Organisation of processes, activities and measures that are activated when necessary to prevent, limit or manage the risks of failure or disruption of a service during the period until normal operation is restored.

2) Cyber Security: The activities necessary to protect network and information systems, users of such systems and other persons affected by cyber threats.

3) Supply-critical network and information system: A network and information system capable of directly interrupting or influencing physical and logical processes necessary for providing supply to one or more end-users, including industrial control systems, operational technologies and network and information systems directly integrated with them.

4) Incident: An incident that has the potential to significantly interfere with or which interferes with the provision of an essential service, including when it affects national systems ensuring the rule of law and including events that jeopardise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by or accessible through network and information systems.

5) Managing an incident: Any action and procedure aimed at preventing, detecting, analysing and suppressing or responding to and re-establishing operations after an incident.

6) Industrial control systems: Network and information systems used for all forms of digital management, control and monitoring of physical and industrial processes, such as the management, control and monitoring of valves and pumps or the collection and analysis of data from a physical system, including sensors and control components connected to an industrial network environment.

7) Management body: the central management body as defined in the Danish Companies Act and the management body as defined in the Danish Act on Certain Commercial Undertakings, respectively, depending on the enterprise's corporate form.

8) Network and information system:

a) An electronic communication network that supports transmission systems, whether or not they are built on a permanent infrastructure or centralised management capacity and, where appropriate, interconnection and routing equipment and other resources, including non-active network elements which enable transmission of signals by means of wiring, radio waves, light conductor technology or other electromagnetic means, including satellite networks, terrestrial fixed and mobile networks, electric cable systems, to the extent that they are used for transmission of signals, networks used for radio and television distribution, and cable television networks, regardless of the type of information transmitted.
b) Any device or group of connected or related devices, one or more of which automatically process digital data by means of a program.
c) Digital data stored, processed, retrieved or transmitted by elements referred to in points (a) and (b) for their operation, use, protection and maintenance.

9) Operational technologies: Physical network and information systems monitored or controlled by industrial control systems.

10) Risk: The potential for loss or disruption as a result of an incident, expressed as a combination of the magnitude of such loss or disruption and the probability of the incident occurring.

11) Risk assessment: The overall process for determining the nature and extent of a risk by identifying and analysing potentially relevant threats, vulnerabilities and dangers that could lead to an incident and by evaluating the potential loss or potential disruption to the provision of an essential service caused by that incident.

12) Security of network and information systems: The ability of networks and information systems to withstand, at a given level of security, any incident that may impair the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by or accessible through those networks and information systems.

13) Vulnerability: A weakness, susceptibility or error of processes, products, services, physical devices and the like that may affect the likelihood that an incident may occur.

Chapter 2

Level division of enterprises and classification of plants

Section 4. Enterprises are divided into five levels according to the thresholds in Annex 1.

(2) The Danish Energy Agency decides on the level division of an enterprise on the basis of its activities and its importance to the overall supply of the subsector in question at the local, regional, national or European level.

(3) Enterprises operating within several subsectors shall be assigned the highest level, cf. the thresholds set out in Annex 1. This is assessed separately for each commercial law entity with a separate CVR number.

(4) Enterprises that jointly carry out preparatory work in a coordinated emergency facility, cf. Section 113, shall be assigned the same level. The Danish Energy Agency shall include in the decision the relationship between the operations in the provision of services and their overall importance for the overall supply in the relevant subsectors according to Section 113.

(5) The Danish Energy Agency may decide that an activity should be assigned a higher level than that indicated in the thresholds set out in Annex 1 if special circumstances cause that enterprise to provide its service to end-users which constitute critical units in other sectors.

Section 5. Subject to the provisions of this Executive Order, enterprises classified as Level 1 under Section 4(1 & 2) shall comply only with the provisions of Chapters 15-17 and 19-20, as well as Sections 4, 5, 9, 19(1-5) and Section 73(1, 3 & 4).

Section 6. The plants of enterprises are divided into five classes according to the threshold values set out in Annex 2.

(2) The Danish Energy Agency decides on the classification of an enterprise's plant based on its function and importance for the overall supply in the sub-sector in question at the local, regional, national or European level.

(3) Plants used in several subsectors shall be classified in the highest class, cf. the thresholds set out in Annex 2.

(4) Combined plants are considered as one plant and classified according to the plant with the highest classification.

(5) The Danish Energy Agency may decide that an enterprise's plant is to be classified in a higher class than that indicated in the thresholds set out in Annex 2 if the particular circumstances of that plant may affect the provision of a business service to end-users that constitute critical infrastructure in other sectors.

(6) The Danish Energy Agency may give advance commitments regarding the expected classification of a plant when establishing, assembling and changing a plant. The Danish Energy Agency's advance commitment is binding, provided that the facts on which the commitment is based do not change.

Section 7. The general office facilities of the enterprise used for the provision of the enterprise's services shall comply with the requirements of Section 36(1 & 2), Section 38(1) Section 38(2) no. 1 and 2 and Section 38(3).

Section 8. Plants of enterprises that do not meet the thresholds in Annex 2 are not classified by the Danish Energy Agency pursuant to Section 6.

(2) The measures set out in Chapter 10 shall not apply to class 1 plants.

Section 9. Every three years on 1 October, enterprises shall submit to the Danish Energy Agency the information referred to in Annex 3 which is necessary for the level division of enterprises, cf. Section 4, and the classification of plants, cf. Section 6. However, the first submission of information shall take place on 1 April 2025.

(2) Enterprises shall send information without undue delay about changes in conditions of importance to the level division of an enterprise and the class of a plan

(3) The Danish Energy Agency may require an enterprise to send missing information within a specified period of at least one week for use for decisions pursuant to Section 4(2) and Section 6(2).

(4) Within the electricity and district heating sector, the Danish Energy Agency communicates information on the assigned level of enterprises and the assigned class of enterprise plants to the Danish Energy Agency.

Chapter 3

Roles and responsibilities

Section 10. The risk management and emergency preparedness of enterprises shall be determined by the management body of the enterprise, which shall approve the following:

1) Risk and vulnerability assessments pursuant to Section 18.

2) Risk assessments in connection with projects to be submitted to the Danish Energy Agency pursuant to Section 28(1).

3) Emergency response plans pursuant to Section 19.

Section 11. Enterprises shall have one emergency coordinator to coordinate emergency planning, including assisting in the preparation of risk and vulnerability assessments pursuant to Section 18 and emergency plans pursuant to Section 19.

(2) Enterprises shall have one cyber coordinator to coordinate measures to support the security of network and information systems and assist in the emergency planning of their network and information systems.

(3) Enterprises with plants in classes 4 and 5 shall have one or more security coordinators to coordinate actions at their plants in classes 4 and 5.

(4) The emergency coordinator, cyber coordinator and security coordinator shall coordinate in the different areas between each other so that the enterprise's preparedness is planned based on a comprehensive risk picture.

(5) The management body of the enterprise shall meet at least four times a year with the coordinating roles referred to in sub-sections 1 to 3 in order to take a position on the organisation's risk preparedness, physical security and cybersecurity. Minutes shall be taken of the meetings.

(6) Enterprises at levels 4 and 5 shall not have the same people in the role of the emergency coordinator, the cyber-coordinator and the management body of the company that approves risk assessments and emergency plans pursuant to Section 10.

(7) Enterprises shall notify the Danish Energy Agency of updated contact details on the coordinating roles referred to in sub-sections 1-3.

Chapter 4

Risk management policy

Section 12. Enterprises shall have policies for risk management or the equivalent to set the framework for their risk management work. The policies shall include the following:

1) Description of management responsibilities and roles.

2) Methods for identifying, assessing and evaluating risks, including risks to plants and networks and information systems.

3) Methods for identifying, assessing, managing and prioritising appropriate measures to mitigate and manage risks.

4) Criteria for the assessment and prioritisation of risk.

5) Criteria for risk tolerance.

Chapter 5

Emergency response planning

Section 13. Enterprises shall undertake emergency response planning so that the enterprise's emergency response plans pursuant to Section 19 ensure operational continuity and so the enterprise can comply with its notification obligations in the event of an incident.

(2) Enterprises shall address the need for redundancy, including redundancy of network and information systems and plants used in the provision of their services.

(3) Enterprises shall participate in national crisis management, including translating notifications of changes in security preparedness levels and sectoral preparedness measures into necessary actions within their own organisation without undue delay.

(2) Enterprises shall have one cyber coordinator to coordinate measures to support the security of network and information systems and assist in the emergency planning of their network and information systems.

(3) Enterprises with plants in classes 4 and 5 shall have one or more security coordinators to coordinate actions at their plants in classes 4 and 5.

(4) The emergency coordinator, cyber coordinator and security coordinator shall coordinate in the different areas between each other so that the enterprise's preparedness is planned based on a comprehensive risk picture.

(5) The management body of the enterprise shall meet at least four times a year with the coordinating roles referred to in sub-sections 1 to 3 in order to take a position on the organisation's risk preparedness, physical security and cybersecurity. Minutes shall be taken of the meetings.

(6) Enterprises at levels 4 and 5 shall not have the same people in the role of the emergency coordinator, the cyber-coordinator and the management body of the company that approves risk assessments and emergency plans pursuant to Section 10.

(7) Enterprises shall notify the Danish Energy Agency of updated contact details on the coordinating roles referred to in sub-sections 1-3.

Records

Section 14. Enterprises shall keep up-to-date records of the plants necessary for the enterprise to provide its services.

(2) The records referred to in sub-section 1 shall describe the function of a plant in the provision of the enterprise's services, its criticality for the provision of its services, its geographical location and any potential dependencies on spare parts, networks and information systems and suppliers.

(3) Records referred to in sub-section 1 shall contain information on the dependence of the enterprise on other enterprises in the provision of its services.

Section 15 Enterprises shall keep up-to-date records of the network and information systems used by the enterprise in the provision of its services.

(2) The records referred to in sub-section 1 shall describe the processes supported by a network and information system, its criticality for the provision of services to the enterprise, internal positioning of responsibilities, lifetime and potential dependence on other network and information systems and suppliers.

(3) Records referred to in sub-section 1 shall contain information on the dependence of the enterprise on internal and external network and information systems in the provision of its network networks.

Section 16. Enterprises shall keep a record of physical and digital information flows that form part of the communication between management-critical functions in the provision of their services and which the enterprise sends and receives from external actors and external network and information systems.

(2) The records referred to in sub-section 1 shall include an assessment of the risks of loss of confidentiality, integrity and accessibility of the mentioned information flows.

Section 17. Records according to Sections 14-16 shall be kept up to date, so that the records are always accurate.

Risk and vulnerability assessment

Section 18. Enterprises shall conduct a risk and vulnerability assessment of known and potential risks that may interfere with or prevent the provision of their services.

(2) The risk and vulnerability assessment referred to in sub-section 1 shall include:

1) An identification and assessment of risks and vulnerabilities.

2) An assessment of the impacts of potential incidents, including potential derived societal consequences.

3) A risk management action plan which specifies:

a) The measures to mitigate and manage risks and vulnerabilities, including measures referred to in Chapters 10 and 11.
b) A schedule for the implementation of the measures referred to in point (a).
c) An internal assignment of responsibilities for the implementation of the requirements in point (a).

(3) As part of their identification and analysis of risks and vulnerabilities, enterprises shall:

1) Take into account the Danish Energy Agency's risk and vulnerability scenarios, cf. Section 107(5).

2) Include relevant sources of information, including the enterprise's own experience as well as threat and vulnerability assessments from authorities and IT security officials, cf. Section 33(1).

3) Take into account risks which are deemed to remain after the enterprise has implemented measures pursuant to sub-section 2, no. 3, point (a).

(4) The risk and vulnerability assessment pursuant to sub-section 1 shall be carried out with the participation of relevant staff and suppliers with technical and organisational knowledge of the enterprise's processes, plants, network and information systems, network infrastructure and supplier relations.

(5) The risk and vulnerability assessment pursuant to sub-section 1 shall be updated with material changes and incorporated into the overall risk picture of the enterprise.

(6) The measures pursuant to sub-section 2, no. 3 shall be implemented taking into account the current technical level, implementation costs and the severity of the risks.

Emergency response plans

Section 19. Enterprises shall have management-approved, cf. Section 10, emergency response plans for incident management and crisis management. Emergency response plans may include one or more sub-emergency plans, procedures and instructions.

(2) The emergency response plans pursuant to sub-section 1 shall at minimum describe:

1) The internal distribution of responsibilities and roles, including monitoring and establishing a crisis staff or crisis management body relevant to the handling of an incident.

2) Opportunities to activate additional resources and material, including additional operational personnel and support from other enterprises under contracts or other agreements.

3) The operational responsibility distribution between the enterprise and its business partners or suppliers in connection with the handling of an incident.

4) The contact details of relevant persons in connection with the handling of an incident, including operators and system operators as well as emergency staff.

5) The criteria for activating a crisis management group for handling an incident.

(3) The emergency response plans pursuant to sub-section 1 shall contain the following procedures:

1) Procedures for the establishment of alternative operations in the event of failures in processes, plants and network and information systems, including descriptions of:

a) Options for switching to manual operation.
b) Methods and conditions for activating redundant network and information systems and emergency processes.

2) Procedures for isolating industrial control systems and operational technologies, including a description of methods for isolating the systems and conditions for activating the plans.

3) Procedures for restoration of a plant, including a description of how quickly spare parts, personnel and other resources can be acquired to restore operation in the event of damage to the parts of the plant essential for the operation of the enterprise.

4) Procedures for obtaining critical spare parts from the enterprise's own warehouse or from suppliers.

5) Procedures for the restoration of network and information systems, including descriptions of:

a) Maximum accepted downtime and data loss for network and information systems.
b) The target for restoration time and methods to restore network and information systems from backups.
c) Conditions for activating procedures for recovery.

6) Procedures for the implementation of emergency response measures which may be implemented in connection with the handling of an incident, including sectoral emergency response measures.

7) Procedures for exchanging operational critical information in the event of a breakdown of normal communication lines in connection with an incident.

8) Procedures for documenting the enterprise's handling of an incident.

9) Procedures for receiving, obtaining, processing and sharing relevant information within the enterprise in connection with the handling of an incident.

10) Procedures for external information sharing on incidents and incident handling to relevant institutions, business partners, consumers, the press, the public and other actors.

(4) The emergency response plans pursuant to sub-section 1 shall be consistent with the sectoral emergency response plans for the subsector in which the enterprise operates.

1) The operational responsibility distribution between the enterprise and its business partners or suppliers in connection with the handling of an incident.

2) The contact details of relevant persons in connection with the handling of an incident, including operators and system operators as well as emergency staff.

3) The criteria for activating a crisis management group for handling an incident.

(5) The emergency response plans pursuant to sub-section 1 shall contain the following procedures:

1) Procedures for the establishment of alternative operations in the event of failures in processes, plants and network and information systems, including descriptions of:

a) Options for switching to manual operation.
b) Methods and conditions for activating redundant network and information systems and emergency processes.

2) Procedures for isolating industrial control systems and operational technologies, including a description of methods for isolating the systems and conditions for activating the plans.

3) Procedures for restoration of a plant, including a description of how quickly spare parts, personnel and other resources can be acquired to restore operation in the event of damage to the parts of the plant essential for the operation of the enterprise.

4) Procedures for obtaining critical spare parts from the enterprise's own warehouse or from suppliers.

5) Procedures for the restoration of network and information systems, including descriptions of:

a) Maximum accepted downtime and data loss for network and information systems.
b) The target for restoration time and methods to restore network and information systems from backups.
c) Conditions for activating procedures for recovery.

6) Procedures for the implementation of emergency response measures which may be implemented in connection with the handling of an incident, including sectoral emergency response measures.

7) Procedures for exchanging operational critical information in the event of a breakdown of normal communication lines in connection with an incident.

8) Procedures for documenting the enterprise's handling of an incident.

9) Procedures for receiving, obtaining, processing and sharing relevant information within the enterprise in connection with the handling of an incident.

10) Procedures for external information sharing on incidents and incident handling to relevant institutions, business partners, consumers, the press, the public and other actors.

(6) The emergency response plans pursuant to sub-section 1 shall be consistent with the sectoral emergency response plans for the subsector in which the enterprise operates.

(7) Emergency response plans pursuant to sub-section 1 shall be version-management with a brief description of the changes in relation to previous versions.

(8) The emergency response plans pursuant to sub-section 1 shall take into account the conclusions of the risk and vulnerability assessment, cf. Section 18, and shall, where necessary, be updated in connection with the conduct of a risk and vulnerability assessment.

Exercises and functional tests

Section 20 Enterprises shall have a plan for exercises that the enterprise plans to carry out over a five-year period in accordance with Section 21.

(2) The five-year exercise plan shall cover all exercise elements specified in Annex 4.

(3) Initially, enterprises shall draw up a five-year exercise plan covering the period from 1 October 2025 to 30 September 2030. A new exercise plan shall then be prepared for a new five-year period.

(4) The five-year exercise plan is provisional and shall be updated at least once a year and with material changes.

Section 21 Enterprises at level 3-5 shall practice their emergency response plans at least once a year based on their own emergency response plans, cf. Section 19.

(2) Level 2 enterprises shall practice their emergency response plans at least every two years.

(3) Level 4 and 5 enterprises shall practice once a year the restoration of their critical supply network and information systems, cf. practice element no. 18 in Annex 4.

(4) The management body of the enterprise shall, where appropriate, participate in the emergency response exercises.

(5) Enterprises shall, at the request of either Energinet or the Danish Energy Agency, participate in sector emergency response exercises, cf. Section 89 and Section 101.

Section 22 Enterprises shall conduct annual functional testing of technical equipment which the enterprise plans to use in the handling of an incident, including testing of alternative means of communication and technical controls for communication routes.

Section 23 Enterprises shall evaluate exercises carried out by the enterprise pursuant to Section 21.

(2) Enterprises shall prepare and send an exercise evaluation when the exercise has contained exercise elements from Annex 4 to the Danish Energy Agency for approval within three months after the exercise has been held. The exercise evaluation shall contain at minimum a description of:

1) Trained exercise elements, cf. Annex 4.

2) The course of the exercise.

3) Acquired experiences.

4) Relevant learning outcomes.

5) A scheduled follow-up on the learning outcomes in No. 4, including a schedule and internal positioning of responsibilities for the follow-up process.

(3) The Danish Energy Agency may forward relevant learning outcomes from an enterprise in the exercise assessment of the electricity, gas or hydrogen sector pursuant to sub-section 2, no. 4 to the Danish Energy Agency if the Danish Energy Agency considers it necessary for the Danish Energy Agency's ability to carry out the coordination tasks of the sectoral emergency response, cf. Section 81.

(4) The Danish Energy Authority may share relevant learning outcomes from an enterprise's exercise evaluation with other enterprises and authorities in an anonymous form if the Danish Energy Authority considers it relevant for the emergency response plans of the sector as a whole.

(5) The Danish Energy Agency shall consult the enterprise in question if the learning outcomes are scheduled to be forwarded before the forwarding may take place pursuant to sub-sections 3 and 4.

Chapter 6

Teaching and awareness

Section 24 Members of an enterprise's management body shall attend relevant courses or training on organisational risk preparedness, physical security and cybersecurity.

Section 25 Enterprises shall ensure that persons carrying out tasks in the fields of organisational preparedness, physical security and cybersecurity build up and maintain the necessary competencies, including receiving the necessary instruction, teaching and training.

Section 26 Enterprises shall conduct annual awareness initiatives to promote and maintain awareness of relevant emergency response plans, threats and vulnerabilities within the enterprise.

(2) Enterprises shall implement awareness-raising measures annually to promote and maintain their ability to identify and address relevant cyber threats and vulnerabilities.

Chapter 7

Risk assessments of projects

Section 27 Enterprises shall carry out a risk assessment in accordance with Section 18(1, 2 & 4) in connection with the following projects:

1) The acquisition and development of supply-critical networks and information systems.

2) The establishment of new plants or the acquisition of plants in class 3 to 5 in accordance with the thresholds specified in Annex 2. Changes being made to existing plants of class 3 to 5 which are expected to result in a change in the classification of a plant, cf. the thresholds specified in Annex 2.

3) The outsourcing of development, operation and maintenance tasks that may affect the delivery of the enterprise's services.

(2) Risk assessments pursuant to sub-section 1 where a supplier relationship is included shall include an assessment of the risks arising from the supplier relationship, cf. the procedures in Section 29.

(3) Risk assessments pursuant to sub-section 1 shall be prepared at the start of the project and submitted in writing before the start of the project. The risk assessment shall be updated when the scope, schedule and partial deliveries of the project are changed to such an extent that they change the prerequisites for the risk assessment.

Section 28 Risk assessments pursuant to Section 27 shall be submitted to the Danish Energy Agency for approval in connection with the following projects:

1) Construction projects referred to in Section 27(1), no. 2 and 3, where a plant at completion is expected to meet the thresholdfor plants of classes 4 and 5, cf. the thresholds specified in Annex 2.

2) Acquisition or development of supply-critical network and information systems pursuant to Section 27(1), no. 1 and 3.

(2) Risk assessments pursuant to sub-section 1 shall be submitted to the Danish Energy Agency within one month of the approval by the management body of a risk assessment, cf. Section 10, no. 2.

(3) Projects pursuant to Section 27 may be implemented until the final approval of the risk assessment by the Danish Energy Agency, cf. sub-section 1, is completed.

Chapter 8

Supplier management and supply chain security

Section 29 Enterprises shall have procedures for supply chain security in supplier relationships so that the enterprise takes appropriate and proportionate measures in relation to the products and services used by the enterprise to provide its services. The procedures shall include:

1) Methods for identifying, assessing and managing risks that are specific to each direct supplier and service provider in the supply chain, including risks associated with subcontractor dependencies and international conditions in an agreement with a direct supplier and service provider.

2) Methods for assessing the resilience of the delivery of products and services, including the general quality of any potential integrated measures to manage risks in network and information systems.

Section 30 When entering into contracts with direct suppliers and service providers of products and services that may affect the security of supply or the security of their network and information systems, enterprises shall ensure:

1) That there are requirements for appropriate measures to manage risks and deal with incidents in relation to the products and services provided.

2) That the enterprise is notified of material incidents, cf. Section 77(2), as regards the products and services supplied by the direct supplier or service provider.

3) That the direct supplier or service provider assists the enterprise in complying with its reporting obligations in the event of material incidents, cf. Sections 77-80.

4) That direct suppliers and service providers may be involved in the connection of the Danish Energy Agency's supervision of the enterprise regarding compliance with the provisions of the Act on Enhanced Preparedness in the Energy Sector and this Executive Order.

5) That direct suppliers commit to participating, as appropriate, in the enterprise's exercises, cf. Annex 4, no. 13 and 14.

6) That direct suppliers and service providers can be involved in the enterprise's emergency response work where appropriate.

7) That there is specified criteria for direct suppliers offering substantial parts of a supplier contract to one or more subcontractors.

8) That the enterprise, in relation to direct suppliers and service providers, retains ownership of data which is necessary for the provision of the enterprise's service or which is confidential, cf. Section 26 of the Act on Enhanced Preparedness in the Energy Sector.

Section 31 Enterprises shall have procedures for controlling remote access for direct suppliers and service providers who can access their enterprise's supply-critical network and information systems.

(2) If a direct supplier or service providers need remote access to the enterprise's supply-critical networks and information systems, the procedures shall be specified in the supplier agreement.

Section 32 Enterprises shall ensure that requirements regarding organisational preparedness, physical security and cybersecurity directed at direct suppliers or service providers pursuant to Section 30 and Section 31 are specified in a supplier agreement.

(2) Enterprises shall ensure that direct suppliers and service providers can demonstrate to the enterprise compliance with requirements set out in a supplier contract, cf. Sections 30 and 31.

Chapter 9

IT security service

Section 33 Enterprises shall have a registered IT security officer who shall notify the enterprise of relevant vulnerabilities and cyber threats without undue delay and guide the enterprise on the effectiveness of mitigating measures.

(2) The supplier agreement with an IT security service shall specify how quickly the IT security service shall notify the enterprise when vulnerabilities and cyber threats are detected.

(3) Enterprises shall ensure that the IT security service has the necessary knowledge of the enterprise's network and information systems so that the IT security service can identify and alert the enterprise to relevant vulnerabilities and cyber threats.

(4) Enterprises shall ensure that warnings are received by persons with the necessary competencies to convert warnings into mitigating action within the enterprise taking into consideration the seriousness of a warning.

(5) Enterprises that enter into a joint contract with an IT security service shall all be identified in the contract with the IT security service. The contract shall be stored with all registered enterprises.

Section 34 Enterprises at level 3 to 5 shall ensure that an IT security service assists the enterprise in handling an incident, including that the IT security service can provide assistance for damage mitigation, evidence collection and technical assistance to restore network and information systems.

Section 35 Companies shall ensure that information about vulnerabilities and incidents obtained through their IT security services can be passed on to other enterprises without undue delay.

Chapter 10

The resilience of plants

Section 36 Enterprises shall have appropriate and proportionate measures to ensure that their plants are resilient to damage and loss of functions.

(2) Enterprises shall carry out appropriate and proportional climate adjustments to their plants so that they are resilient to damage or functional losses due to climate-related incidents.

(3) Enterprises shall at minimum have measures in place to support the following for their plants in Class 3 to 5, however, cf. sub-section 4:

1) That damage or defects to the plants are detected, verified and notified of.

2) That the plant is resistant to functional failures of networks and information systems.

3) That the plant is resistant to functional failures of publicly tendered electronic communications networks or services.

(4) Transmission system operators and distribution system operators in the electricity sector shall have the measures referred to in sub-section 3 implemented for plants in class 2-5.

(5) For plants of class 3 to 5, enterprises shall have an emergency power supply which, in the event of power outage, ensures that the plant is not damaged during shutdown and is functional when the power supply is restored, however, cf. sub-section 6.

(6) Transmission system operators and distribution system operators in the electricity sector shall, for plants in:

1) Class 4 and 5 have an emergency power supply, which in case of power outages ensures the functionality of the plant for a period of time until the power supply is restored.

2) Class 3 have an emergency power supply, which in case of power outages ensures the functionality of the plant for a minimum of 24 hours.

3) Class 2 have an emergency power supply, which in case of power outages ensures the functionality of the plant for a minimum of 4 hours.

(7) Enterprises shall ensure that functional losses and damage to plants are remedied so that the enterprise can restore its ability to provide its services without unnecessary delays.

(8) At least every six months, enterprises shall check that the measures referred to in sub-sections 2-4 and 7 and 10 are implemented, intact and function as intended.

(9) At least every year, enterprises shall carry out the emergency power testing on a plant, cf. sub-sections 5 and 6.

(10) In the case of construction projects, enterprises shall on the basis of a risk assessment have appropriate and necessary measures to ensure the resilience of the plant during the construction phase.

Section 37 Enterprises shall have a system for managed access control so that only authorised and verified persons can access their plants.

(2) Enterprises shall determine which employees and suppliers may and can have access to different parts of their plants, including the possibility of unaccompanied access to the plants or parts thereof.

(3) Enterprises shall ensure that guests and other persons who do not have a fixed work schedule on a plants or parts of the plant are included in the managed access control system.

(4) Enterprises shall ensure that accesses are logged so that personally identifiable logs on accesses to their plants can be documented. The documentation shall be protected as described in Section 67.

(5) At least every six months, enterprises shall check that the managed access controls referred to in sub-sections 1-4 are carried out, are intact and function as intended, including checking that only authorised persons have access to the plants of the enterprise.

(5) Based on a risk assessment, levels 4 and 5 enterprises shall visually shield areas and equipment that can provide insight into critical energy infrastructure, including visually shielding control rooms.

(6) Enterprises shall verify that the procedures pursuant to sub-sections 2 to 5 are carried out, are intact and function as intended, including inspecting and testing the physical security of the plant. The inspection of plants of classes 2 and 3 shall be carried out on a quarterly basis. The inspection of class 4 and 5 plants shall be carried out on a monthly bas

Section 37 Enterprises shall have a system for managed access control so that only authorised and verified persons can access their plants.

(2) Enterprises shall determine which employees and suppliers may and can have access to different parts of their plants, including the possibility of unaccompanied access to the plants or parts thereof.

(3) Enterprises shall ensure that guests and other persons who do not have a fixed work schedule on a plants or parts of the plant are included in the managed access control system.

(4) Enterprises shall ensure that accesses are logged so that personally identifiable logs on accesses to their plants can be documented. The documentation shall be protected as described in Section 67.

(5) At least every six months, enterprises shall check that the managed access controls referred to in sub-sections 1-4 are carried out, are intact and function as intended, including checking that only authorised persons have access to the plants of the enterprise.

Section 38 Enterprises shall have measures to ensure that attempts of unauthorised access to their plants are prevented, detected and responded to.

(2) The measures referred to in sub-section 1 shall at minimum include:

1) Managed access control, cf. Section 37.

2) Security measures to delay and hinder physical entry into the plant.

3) Electronic surveillance to detect attempted intrusion, including attempted sabotage, burglary or theft.

4) Electronic monitoring to verify attempts to penetrate class 4 and 5 plants.

(3) Security measures pursuant to sub-section 2 shall also include a general perimeter security so that unauthorised persons, vehicles or vessels on the water cannot be allowed to move into the perimeter of a plant without being detected. For plants forming part of an office building and ordinary office facilities used for the provision of its services, instead of perimeter security there can instead be used building shell security, cf. sub-sections 1 and 2.

(4) For plants of classes 4 and 5, enterprises shall implement cell or object security of areas with access to supply-critical network and information systems, workstations, critical plant components and network equipment that can access supply-critical network and information systems, including control rooms, server rooms and data centres.

(5) Based on a risk assessment, levels 4 and 5 enterprises shall visually shield areas and equipment that can provide insight into critical energy infrastructure, including visually shielding control rooms.

(6) Enterprises shall verify that the procedures pursuant to sub-sections 2 to 5 are carried out, are intact and function as intended, including inspecting and testing the physical security of the plant. The inspection of plants of classes 2 and 3 shall be carried out on a quarterly basis. The inspection of class 4 and 5 plants shall be carried out on a monthly basis.

Section 38 Enterprises shall have measures to ensure that attempts of unauthorised access to their plants are prevented, detected and responded to.

(2) The measures referred to in sub-section 1 shall at minimum include:

5) Managed access control, cf. Section 37.

6) Security measures to delay and hinder physical entry into the plant.

7) Electronic surveillance to detect attempted intrusion, including attempted sabotage, burglary or theft.

8) Electronic monitoring to verify attempts to penetrate class 4 and 5 plants.

(3) Security measures pursuant to sub-section 2 shall also include a general perimeter security so that unauthorised persons, vehicles or vessels on the water cannot be allowed to move into the perimeter of a plant without being detected. For plants forming part of an office building and ordinary office facilities used for the provision of its services, instead of perimeter security there can instead be used building shell security, cf. sub-sections 1 and 2.

(4) For plants of classes 4 and 5, enterprises shall implement cell or object security of areas with access to supply-critical network and information systems, workstations, critical plant components and network equipment that can access supply-critical network and information systems, including control rooms, server rooms and data centres.

(5) Based on a risk assessment, levels 4 and 5 enterprises shall visually shield areas and equipment that can provide insight into critical energy infrastructure, including visually shielding control rooms.

(6) Enterprises shall verify that the procedures pursuant to sub-sections 2 to 5 are carried out, are intact and function as intended, including inspecting and testing the physical security of the plant. The inspection of plants of classes 2 and 3 shall be carried out on a quarterly basis. The inspection of class 4 and 5 plants shall be carried out on a monthly basis.

Section 39 Enterprises shall have procedures for handling alarms notifying of illegal intrusions into their plants so that alarms are handled quickly and in a qualified manner.

(2) Attempts to enter a plant shall be alerted of without undue delay to a 24-hour control room or a control centre approved by the Danish National Police.

(3) Enterprises shall verify quarterly that the alarm handling procedures referred to in sub-sections 1 and 2 are implemented effectively.

Section 40 Enterprises shall have a plan for when the enterprise intends to carry out controls of the security measures of a plant within one year, cf. Section 36(8 & 9),

Section 37(5), Section 38(6), Section 39(3), Section 42(2) and Section 43(2).

(2) Errors and shortcomings in the measures shall be corrected promptly and the reasons for them shall be investigated.

(3) Enterprises shall keep records of completed controls. The control records shall contain at least the following information:

1) Where the control was carried out.

2) When the control was carried out.

3) How the control was carried out.

4) Errors and deviations that were found.

5) How and when errors and deviations were corrected.

(4) When errors and deviations cannot be remedied within a short time, enterprises shall draw up a plan for how and when the error or deviation will be finally remedied.

(5) At the subsequent control, enterprises shall ensure that errors and deviations from the previous control are checked again so that it can be determined that the remedial measures are working as intended.

Section 41 Enterprises shall implement measures pursuant to Sections 36-39 on plants which are built together with other plants, regardless of the combination, according to the plant with the highest class.

Section 42 For pipelines and cables that are dug down, hanging in the air, lying on or buried in the seabed, enterprises shall only implement measures pursuant to Section 36(1 & 2) and ensure that the plant is monitored so that malfunctions are detected and responded to without unnecessary delay.

(2) At least every six months, enterprises shall check that the measures referred to in sub-section 1 are implemented, intact and function as intended.

Section 43 Enterprises shall have appropriate and proportionate measures to ensure that attempts at intrusion and unauthorised access to their plants, locations, facilities that are not classified but where critical components of the plant or network equipment able to access network and information systems are stored are detected and alerted of without unnecessary delay to a 24-hour manned control room or a control centre approved by the Danish National Police.

(2) Enterprises shall conduct spot checks to ensure that the measures referred to in sub-section 1 are implemented, are intact and function as intended, cf. Section 40(2 & 3).

Chapter 11

Security of network and information systems

Section 44 Enterprises shall have an information system security policy to define a general framework for the security of their network and information systems.

Section 45 Enterprises shall have security procedures in place for the acquisition, development and maintenance of network and information systems. The procedures shall include the following:

1) Requirements to maintain an appropriate level of security in network and information systems that an enterprise acquires, develops and maintains, including security requirements in development and testing environments.

2) Methods to verify that the network and information systems acquired or deployed meet the operational requirements of no. 1.

Section 46 Enterprises shall ensure that their network and information systems as well as software and hardware assets used in the provision of their services are hardened, to the extent possible, including through secure configurations as described in Section 49 and with anti-malware and the latest system and security updates throughout their lifecycle.

(2) System and security updates of supply-critical networks and information systems pursuant to sub-section 1 shall be revised on the basis of a risk assessment in which the risks to the security of the systems are evaluated in relation to the risks of the ability of the enterprise to maintain its ability to deliver its services.

Section 47 Enterprises shall be able to identify, respond to and mitigate vulnerabilities that may affect the security of their network and information systems.

(2) Enterprises shall be able to receive vulnerability notifications electronically.

(3) On receipt of a vulnerability notice, enterprises shall carry out a risk assessment of their exposure and mitigate vulnerabilities that may affect the security of their network and information systems.

(4) Level 4 and 5 enterprises shall be able to respond to notifications pursuant to sub-sections 2 and 3 without undue delay.

(5) Enterprises shall decide whether vulnerabilities identified by them in their network and information systems should be disclosed, including in connection with the acquisition, development and maintenance of network and information systems, cf. Section 45.

(6) Enterprises shall ensure that information about vulnerabilities that may have security implications for the energy sector is passed on to the Danish Energy Agency. Enterprises in the electricity, gas and hydrogen sectors shall also forward information on vulnerabilities to Energinet.

Management of software and hardware assets

Section 48 Enterprises shall have updated inventories of the following software and hardware assets:

1) Servers, databases and network equipment used in connection with the provision of the enterprise's services.

2) Endpoints and virtual machines that can access enterprise network and information systems.

3) Software and hardware assets in the enterprise's supply-critical network and information systems.

(2) The lists shall be sufficiently detailed to ensure the rapid identification of an asset so that any vulnerabilities can be identified, assessed and mitigated, cf. Section 47. (3) The enterprises shall regularly and annually as a minimum verify that the records referred to in sub-section 1 are updated. Errors and shortcomings shall be corrected quickly and the reasons for them shall be investigated.

(4) Enterprises shall mitigate risks to software and hardware assets referred to in sub-section 1, no. 1-3, which are used in the delivery of the enterprise's services and which can no longer be supported by system and security updates, cf. Section 46(1).

Section 49 Enterprises shall have procedures to ensure that their network and information systems as well as software and hardware assets pursuant to Section 48 are configured securely, including that functions, services, applications, network protocols and ports that are not necessary to provide the services of the enterprise are closed or disabled.

(2) The procedures referred to in sub-section 1 shall include the secure connection of new hardware assets to the networks on which the enterprise is dependent in the provision of its services. (3) Enterprises shall log material configuration changes to their critical supply network and information systems.

(4) Enterprises shall log changes to network equipment used in the segmentation of networks pursuant to Section 62. (5) Enterprises shall regularly and at least annually check that their network and information systems as well as software and hardware assets pursuant to Section 48 are configured pursuant to sub-sections 1-4. Errors and shortcomings shall be corrected quickly and the reasons shall be investigated.

Section 50 Level 4 and 5 enterprises shall place servers and data centres that support their supply-critical network and information systems within EU/EEA country.

Access control

Section 51 Enterprises shall have access control policies to ensure that their network and information systems are protected from unauthorised physical and logical access.

Section 52 Enterprises shall conduct access controls for accesses, identities and rights to their network and information systems. The access control shall support the following:

1) That accesses and rights are personally identifiable and are granted only on a work-related need.

2) That inactive identities, users and service accounts are deactivated and removed.

3) That the assignment, modification and removal of accesses, identities, rights and accounts are systematically logged.

(2) Enterprises shall perform at least a quarterly clean-up of accesses, identities and rights to supply-critical network and information systems.

Section 53 Enterprises shall, as far as possible and when relevant, use multi-factor authentication (MFA) or continuous authentication when accessing their network and information systems, however, cf. Section 55(1).

Section 54 Enterprises shall manage access elements, including passwords for their network and information systems and network equipment that may affect the provision of their services. The access control shall support:

1) That the access elements used correspond to the criticality of the network and information system or network equipment in question.

2) That as far as possible there is a forced change of passwords so that the strength of passwords corresponds to the criticality of the network and information system or network equipment in question.

(2) Enterprises shall make it compulsory to change standard passwords for network and information systems and network tools before they are connected to the enterprise's network, cf. Section 49(2).

Section 55 Enterprises shall ensure that remote access to the network and information systems of the enterprise is protected in accordance with the provisions of Sections 52-54.

(2) Remote access to the enterprise's supply-critical networks and information systems shall be assigned for a limited period of time so that remote accesses are only open for periods of time when there is an approved work-related need to access a system.

(3) Enterprises shall develop procedures to be able to detect and address cyberattacks against remote accesses to supply-critical networks and information systems.

Section 56 Enterprises shall ensure that mobile and stationary devices that have access to their industrial control systems and operational technologies are not used for private use and configured securely, cf. Section 49, so that only applications that are to be used in the provision of the service can be installed on the device.

Section 57 Enterprises shall regularly verify that measures pursuant to Sections 52-56 are implemented and operate as intended. Errors and shortcomings shall be corrected promptly and the causes investigated.

Backup management

Section 58 Enterprises shall have a policy and procedures for the backup management of their network and information systems. The policy shall contain at least the minimum frequency for taking backups as well as appropriate retention times for backups, cf. Section 19(3), no. 5, point (a).

Section 59 Enterprises shall take backups of their supply-critical networks and information systems and network configurations so that the enterprise can restore the systems and network infrastructure of supply-critical network and information systems.

(2) Backups pursuant to sub-section 1 shall be protected and stored in a safe manner in accordance with the critical nature of the supply-critical network and information system or network configuration that is being backed up.

(3) Enterprises at Level 4 and Level 5 shall take backups pursuant to sub-section 1 in multiple copies so that the enterprise can access backups, regardless of whether the supply-critical network and information system or network configuration that is being backed up is inaccessible or compromised. Backups should be stored separately, for example as offline copies.

Cryptography and secured communications

Section 60 Enterprises shall have policies and procedures for the use of cryptography and, where appropriate, encryption shall be used to protect data when data is stored and when data is transmitted between networks.

Section 61 Enterprises shall use secure voice, video and text communications within the enterprise where relevant to protect against incidents.

Network segmentation and network documentation

Section 62 Enterprises shall implement network segmentation so that their supply-critical networks and information systems are isolated from other networks and information systems and equipment.

(2) The network segmentation pursuant to sub-sections 1, 3 and 5 shall be implemented out using a demilitarised zone or area to be placed between the isolated network of supply-critical networks and information systems and other networks.

(3) Enterprises at levels 4 and 5 shall physically separate networks with supply-critical networks and information systems from other networks, however, see sub-section 5.

(4) Utility enterprises supplying multiple utilities at levels 4 and 5 shall ensure that networks with critical supply networks and information systems are separated across types of supply in accordance with sub-section 3, unless it is a critical supply network and information system for the control of a plant providing multiple energy supply services.

(5) Enterprises at levels 4 and 5 shall implement network segmentation for networks and information systems used in the access control of plants, cf. Section 37 and Section 38(2), no. 3 and 4. Networks and information systems can be placed in the same physical networks as supply-critical networks and information systems.

Section 63 Enterprises shall have updated network documentation describing the structure of their network infrastructure, including the network segmentation referred to in Section 62.

(2) Enterprises shall have up-to-date documentation of communication protocols used in network segments with supply-critical networks and information systems, cf. Section 62, including communication protocols adapted to supply-critical networks and information systems.

(3) Enterprises shall regularly and at least annually verify that the documentation pursuant to sub-sections 1 and 2 is updated.

Logging and monitoring

Section 64 Enterprises shall have a log policy to establish a general framework for logging and monitoring in their networks and information systems. The log policy shall contain at least the following:

1) Methods for systematic collection of logs necessary to identify and investigate incidents.

2) Methods for monitoring logs.

3) Responsibility for monitoring of logs.

4) Storage time for the storing of logs.

Section 65 Enterprises at Level 2 and Level 3 shall, where necessary, implement logging and monitoring in their network and information systems and network infrastructure in order to be able to identify incidents and incidents and to support the authorities' investigations.

Section 66 Level 4 and 5 enterprises shall implement logging and monitoring in their network and information systems and network infrastructure in order to be able to identify incidents and incidents in real time and to support authorities' investigations.

(2) Level 4 and Level 5 enterprises shall log at least the following:

1) Places from which data traffic enters and exits enterprise networks, including firewalls and Internet-based services.

2) On hardware and software that support the delivery of the service, including network components and equipment for remote access where possible and the generated logs shall show connections and user actions.

3) On hardware and software supporting access control of a plant, cf. Section 38(2).

Section 67. Logs pursuant to Section 65 and Section 66 shall be time-synchronised and shall be protected by measures that guarantee that logs are kept securely according to the critical nature of the network and information system or network equipment from which logs are collected.

(2) Logs shall be kept separately from the network and information systems and network equipment from which logs are collected and shall be protected against manipulation and against unauthorised access.

(3) Enterprises at levels 4 and 5 shall store logs pursuant to Section 66 for 13 months.

Section 68 Level 4 and 5 enterprises shall be able to respond to irregularities in network and information systems and network infrastructure in real time to ensure that incidents are handled without undue delay.

Section 69 Enterprises shall plan logging and monitoring pursuant to Sections 65-68 in coordination with their IT security service, so that logs relevant to IT security service incident management are collected and monitored.

(2) Level 4 and 5 enterprises shall be able to submit logs to the IT security service within 24 hours.

Section 70 Enterprises shall regularly and at least annually verify that accurate logs of operations are collected from the enterprise's network and information systems and that logs can be used to identify and investigate incidents. Errors and shortcomings shall be corrected quickly and the reasons for them shall be investigated.

Evaluation of the security of network and information systems

Section 71 Enterprises shall develop policies and procedures for assessing the effectiveness of measures implemented by them to support the security of network and information systems pursuant to this Executive

Order and for assessing the need for technical security scans, for example, in the form of vulnerability scans and penetration tests.

Chapter 12

Management of incidents

Section 72 Incidents shall be handled by the individual enterprise based on the enterprise's emergency response plans with the necessary adjustments to the situation.

(2) Enterprises at level 3 to 5 shall be able to deploy sufficient personnel and technical assistance at all times of the day to manage an incident so that the enterprise can maintain or restore its services.

Section 73 Enterprises shall have an operational contact point within their own organisation which authorities and enterprises responsible for sectoral preparedness can contact.

(2) The operational contact point shall be able to receive notifications of changes in sectoral preparedness at any time of the day so that the enterprise can take sectoral preparedness measures in accordance with Section 13(3) and forward information and notifications within the enterprise.

(3) Enterprises shall keep the Danish Energy Agency informed of updated contact information at their operational contact point, however, cf. sub-section 4.

(4) Enterprises in electricity, gas and hydrogen sectors shall keep Energinet informed of updated contact information for their operational contact point.

Section 74 Enterprises shall be able to maintain communication lines or use alternative forms of communication in connection with the handling of an incident.

Notification obligations

Section 75 Enterprises shall notify the recipients of their services without undue delay of material incidents, cf. Section 77, which are likely to negatively affect the provision of their services.

(2) In the notification referred to in sub-section 1, enterprises shall, where possible, state:

1) The expected impacts, actual impacts and the expected duration of the incident.

2) Any potential measures or countermeasures that the beneficiaries of the enterprise's service may take to mitigate risks or impacts arising out of the incident in question.

3) Time periods for when additional information will be provided.

Section 76 Enterprises shall, without undue delay, inform the recipients of their services potentially affected by a significant cyber threat of any potential measures or countermeasures that the recipients may take in response. The enterprises shall also inform the recipients concerned of the significant cyber threat where relevant.

(2) Information on significant cyber threats shall be made available to recipients in an easy-to-understand language.

(3) Enterprises shall not charge the recipient of their services for the provision of notifications pursuant to sub-section 1.

(4) When informing pursuant to sub-section 1, enterprises are not exempt from taking appropriate and immediate measures to prevent or mitigate any potential threat or incident's negative or potentially negative impacts on the recipients of the enterprise's services.

Section 77 Enterprises shall, without undue delay and in all circumstances, notify the Danish Energy Agency of any incident that has a material impact on the provision of their services, however, cf. sub-sections 4 and 5.

(2) Significant incidents pursuant to sub-section 1 include:

1) Incidents which have caused or are likely to cause serious interruptions in the provision of the enterprise's services, including as a result of plant failure, labour market conflicts and failures to deliver which are of essential importance to the society's energy supply.

2) Incidents that have caused or are likely to cause financial loss to the impacted enterprise.

3) Incidents which have affected or are capable of affecting other natural or legal persons by causing significant physical or non-physical harm.

4) Incidents that have triggered or should have triggered the enterprise's emergency response plans, including:

a) Incidents where the confidentiality, integrity, accessibility and authenticity of a network and information systems have been compromised.

b) Incidents where there is a reasonable suspicion or knowledge of breach, theft, sabotage or espionage.

c) Incidents that have required assistance to determine damage to, repair and restore the network and information systems of the enterprise, including assistance from an IT security service, CSIRT and Energinet.

(3) Enterprises shall notify the Danish Energy Agency without undue delay and within 24 hours of having become aware of a material incident. When reporting, the enterprise shall, to the extent possible, provide the following information about the incident:

1) The incident's characteristics, nature or type.

2) The incident's causes and how it transpired.

3) The incident's impacts.

4) Whether the incident is suspected to be caused by illegal or malicious activities.

5) Whether the incident could have had a cross-border effect.

(4) Enterprises shall notify the Danish Energy Agency within 72 hours of becoming aware of a major incident and notify of the status of the incident, including providing an initial assessment of the severity of the incident, its impact and, if possible, the indicators of being compromised.

(5) Enterprises shall notify CSIRT in the event of significant incidents in which the incident has compromised the security of their network and information systems in the same manner as notifications to the Danish Energy Agency pursuant to sub-section 2, no. 1-3, sub-sections 3-4, and section 78(1 & 2).

(6) Enterprises in the electricity, gas and hydrogen sectors shall notify Energinet without undue delay of material incidents pursuant to sub-section 2 in accordance with sub-sections 3-5.

(7) At the request of the Danish Energy Agency or the safety authorities including CSIRT, enterprises shall submit an interim report concerning relevant status updates.

Section 78 Enterprises shall send an incident report to the Danish Energy Agency within one month after the incident notification made pursuant to Section 77(4). The incident report shall contain a detailed description of the incident and the management of the incident by the enterprise, including:

1) The severity and impact of the incident.

2) The number and proportion of users affected by any potential disruption in the provision of the service and the duration of the disruption.

3) The geographical area affected by a potential disruption in the provision of the service.

4) The type of threat or underlying cause that was like to have triggered the incident.

5) Implemented and ongoing mitigating measures.

6) Any potential cross-border effects of the incident.

7) A description of the cooperation with external parties in managing the incident.

8) Acquired experience and learning points from the enterprise's handling of the incident.

9) Planned follow-up on experiences and learning points pursuant to no. 8, including a schedule for follow-ups.

(2) If an incident is ongoing at the time of the incident report referred to in sub-section 1, the enterprise may send a preliminary report with relevant status updates at that time and a final incident report within one month of incident event being managed by the enterprise.

(3) In connection with sub-section 2, enterprises may apply to the Danish Energy Agency to approve the incident evaluation referred to in sub-section 1 as an exercise evaluation, cf. Section 23, if the enterprise has tested specific exercise elements in Annex 4 in the management of the incident. Applications for the approval of an incident as an exercise shall be accompanied by an updated exercise plan, cf. Section 20.

Section 79 Notifications of significant incidents which have compromised the security of the enterprise's network and information systems pursuant to Section 77(1-5) and Section 78(1 & 2), shall be notified to CSIRT and the Danish Energy Agency via the notification solution specified by CSIRT, however, cf. sub-section 2.

(2) Notifications of all other significant incidents pursuant to Section 78 shall be made through the notification solution specified by the Danish Energy Agency.

(3) Applications for the approval of an incident as an exercise pursuant to Section 78(3) shall be sent to the Danish Energy Agency through the application solution indicated by the Danish Energy Agency.

Section 80 Enterprises shall report incidents on land where there is reasonable suspicion or knowledge of burglary, theft, sabotage and espionage to the police.

(2) Enterprises shall report incidents at sea where there is a reasonable suspicion or knowledge of breach, theft, sabotage and espionage to the police and the Danish Defence.

Chapter 13

Energinet's tasks in the context of sectoral preparedness

Section 81 Energinet shall carry out the coordination, planning and operational tasks of the sectoral preparedness before, during and after an incident for the electricity, gas and hydrogen sectors, respectively, including:

1) Gathering and sharing data and information necessary for sectoral preparedness between authorities and enterprises in the fields of electricity, gas and hydrogen, respectively, including data and information of importance to the security of supply.

2) Notify of changes in sectoral preparedness levels and the implementation of sectoral preparedness measures for the electricity, gas and hydrogen sectors, respectively.

3) Handle crisis management by activating sectoral preparedness plans for the electricity, gas and hydrogen sectors, respectively.

(2) In the context of the crisis management pursuant to sub-section 1, no. 3, Energinet shall obtain relevant and updated information concerning, respectively:

1) The situation in the electricity, gas and hydrogen supply systems of neighbouring countries which is of relevance for crisis management in the electricity, gas and hydrogen sectors, respectively.

2) The situation in substantial parts of the domestic grid, including at voltage levels below 100 kV.

3) The situation of substantial parts of domestic gas and hydrogen supply systems, including distribution, production and storage.

(3) In the event of supply disruptions affecting several enterprises in the electricity, gas and hydrogen sectors respectively, the Energinet shall coordinate the crisis management between relevant companies and the Danish Energy Agency, including providing contact information to enterprises and authorities in an emergency situation as well as information on current operating conditions for use by enterprises in handling incidents.

(4) Energinet shall at any time and without undue delay be able to receive and disseminate information of importance for the preparedness from authorities and other actors to relevant enterprises in the electricity, gas and hydrogen sectors, respectively, and to the Danish Energy Agency.

Section 82 Energinet shall establish a formalised cooperation on emergency preparedness conditions in the electricity, gas and hydrogen sectors, respectively, including through knowledge-sharing and meetings on preparedness, physical security and cybersecurity.

Section 83 Energinet shall handle the work for the electricity, gas and hydrogen sectors, respectively, in the local emergency response units established by the police precincts and may involve relevant enterprises in this work. Energinet, together with the Danish Energy Agency, shall be able to take part in the national crisis management work.

Section 84 Energinet may issue emergency response notices regarding the supply of electricity, gas and hydrogen in accordance with an agreement between DR, TV 2/DANMARK A/S, the National Police and the Danish Emergency Management Agency on the procedure for sending emergency notices ('varslingsaftalen', the alert agreement).

Section 85 Energinet shall keep a record of information flows in digital and physical form that are part of critical management functions and decision-making processes in the sector preparedness for the electricity, gas and hydrogen sectors respectively. The record shall contain a comprehensive overview of the mutual relationships of the actors in the supply systems for the electricity, gas and hydrogen sectors respectively and an assessment of the risks of loss of confidentiality, integrity and accessibility of the information flows.

(2) The record shall be kept up to date so that the record is always correct.

Section 86 Energinet shall prepare a sectoral risk and vulnerability assessment for the electricity, gas and hydrogen supply systems in Denmark on 1 March each year, for the first time in 2026.

(2) The sectorial risk and vulnerability assessments referred to in sub-section 1 shall be based on conclusions from risk and vulnerability assessments of enterprises, cf. Section 107, in the electricity, gas and hydrogen sectors respectively. The Danish Energy Agency at the latest by 1 November each year send the conclusions to Energinet.

(3) Sectoral risk and vulnerability assessments shall include risks associated with the mutual relationships of supply systems with relevant overseas supply systems and mutual dependencies.

(4) The Danish Energy Agency may order Energinet to update and send an updated sectoral risk and vulnerability assessment to the Danish Energy Agency in the event of changes in the threat picture or the situation within a specified time limit.

Section 87 Energinet shall draw up sectoral preparedness plans for, respectively, the electricity, gas and hydrogen supply systems in Denmark. The sectoral preparedness plans shall indicate how Energinet plans to manage the crisis response in a coordinated manner. Sectoral preparedness plans shall include:

1) The distribution of responsibilities between enterprises in the electricity, gas and hydrogen sectors and Energinet.

2) A description of how Energinet plans to inform more enterprises in the electricity, gas and hydrogen sectors, respectively, of changes in sector preparedness so that a common situation understanding is achieved among enterprises.

3) Requirements for the form and content of the situation reports provided by enterprises in the electricity, gas and hydrogen sectors shall send to Energinet in connection with the handling of an incident that has activated the sectoral emergency response plans.

4) Description of communication paths, including alternative communication paths and precautions in connection with compromised normal communication paths.

5) Instruction on encryption of information and operational orders.

(2) The sectoral preparedness plans shall be coordinated across the electricity, gas and hydrogen sectors respectively.

(3) The sectoral preparedness plans shall be related to relevant supply systems abroad and coordinated with the relevant system-controlling enterprises abroad.

Section 88 Sectorial preparedness plans pursuant to Section 87 shall be updated within three months of completion or an update of a sectorial risk and vulnerability assessment, cf. Section 86.

(2) Sectorial preparedness plans shall be version-management with a brief description of changes compared to previous versions.

(3) Energinet shall send the updated sector preparedness plans for the electricity, gas and hydrogen sectors respectively to the Danish Energy Agency on 1 April each year, for the first time in 2026.

(4) The Danish Energy Agency shall approve the sectoral preparedness plans for the electricity, gas and hydrogen sectors respectively. Sectoral preparedness plans may be implemented during the approval process.

Section 89 Energinet shall hold sectoral preparedness exercises at least once every two years for the electricity, gas and hydrogen sectors, respectively, based on the sectoral preparedness plans in Section 87.

Section 90 Energinet shall have a plan of sectoral exercises that Energinet plans to implement for the electricity, gas and hydrogen sectors, respectively, over a five-year period. The plan shall be shared with the enterprises concerned.

(2) The five-year exercise plan for sectoral preparedness shall cover at least the exercise elements in no. 1-11, 13-14, 16-17 and 19 of Annex 4.

(3) Initially, Energinet shall prepare a five-year exercise plan for sectoral preparedness covering the period from 1 April 2025 to 31 March 2030. A new exercise plan shall then be prepared for a new five-year period.

(4) The five-year exercise plan for sectoral preparedness is provisional and shall be updated once a year and with material changes.

Section 91 Energinet shall evaluate sector preparedness exercises carried out in accordance with Section 89. Energinet shall involve relevant enterprises in the evaluation process.

(2) Energinet shall prepare and send an exercise evaluation for approval to the Danish Energy Agency within three months after a sector preparedness exercise has been held. The exercise evaluation shall contain the elements described in Section 23(2).

(3) Energinet shall forward the conclusions of the exercise report to enterprises in the electricity, gas and hydrogen sectors, respectively.

Section 92 The Danish Energy Agency may approve that an evaluation of an incident which has activated sectoral emergency response plans for the electricity, gas and hydrogen sectors, respectively, may be included as a sectoral preparedness exercise in the sectoral preparedness exercise plan. In connection with the application, Energinet shall send an updated exercise plan for the sectoral preparedness together with an incident evaluation pursuant to Section 78.

Section 93 Energinet shall conduct annual functional tests of technical equipment which Energinet plans to use in context of the activation of sectoral emergency response plans for the electricity, gas and hydrogen sectors, respectively, including testing of alternative means of communication and technical control of communication paths.

Section 94 Energinet shall, by 1 May each year, submit an annual report to the Danish Energy Agency on the state of emergency preparedness of the electricity, gas and hydrogen sectors respectively, including on the emergency preparedness work of enterprises in the electricity, gas and hydrogen sectors respectively during the previous year.

Chapter 14

The Danish Energy Agency's tasks in connection with the sectoral preparedness

Section 95 The Danish Energy Agency carries out the coordination, planning and operational tasks in the sectoral preparedness before, during and after a crisis for the oil, district heating and district cooling sectors, respectively, including:

1) Collection and sharing of data and information necessary for sectoral preparedness between authorities and enterprises in the oil, district heating and district cooling sectors respectively.

2) Notification of changes in sectoral preparedness levels and the implementation of sectoral preparedness measures for enterprises in the oil, district heating and district cooling sectors, respectively.

3) Crisis management by activating sectoral emergency response plans for the oil, district heating and district cooling sectors, respectively.

(2) In the event of major supply disruptions affecting several enterprises in the oil, district heating and district cooling sectors, the Danish Energy Agency coordinates crisis management efforts with the relevant enterprises.

(3) The Danish Energy Agency shall send, without undue delay, relevant information on emergency response conditions to relevant enterprises in the oil, district heating and district cooling sectors, respectively, and Energinet.

Section 96 The Danish Energy Agency shall establish a formalised cooperation on emergency response conditions in the oil, district heating and district cooling sectors, respectively, including through knowledge-sharing and meetings on emergency response conditions, physical security and cyber security.

Section 97 The Danish Energy Agency shall manage the work for the oil, district heating and district cooling sectors, respectively, in the local emergency response units established by the police precincts and may involve relevant enterprises.

Section 98 The Danish Energy Agency may issue emergency response notices on oil, district heating and district cooling supplies in accordance with an agreement between DR, TV 2/DANMARK A/S, the National Police and the Danish Emergency Management Agency on the procedure for the dispatch of emergency notifications ('varslingsaftalen', the alert agreement).

Section 99 Every year on 1 March, the Danish Energy Agency shall prepare a sectoral risk and vulnerability assessment for the oil, district heating and district cooling systems in Denmark, respectively, and initially in 2026. Sectorial risk and vulnerability assessment shall be drawn up on the basis of conclusions from the risk and vulnerability assessments of operations, cf. Section 107.

Section 100 The Danish Energy Agency shall prepare sectoral preparedness plans for the oil, district heating and district cooling sectors in Denmark. The sectoral preparedness plans indicate how the Danish Energy Authority plans to manage the crisis response in a coordinated manner so that a common understanding of the situation is achieved when changes are made to the sectoral preparedness for the oil, district heating and district cooling sectors respectively.

(2) The Danish Energy Agency shall coordinate, to the extent necessary, the sectoral preparedness plans referred to in sub-section 1 across the oil, district heating and district cooling sectors as well as with the Danish Energy Agency's sectoral preparedness plans pursuant to Section 87.

(3) Sectorial preparedness plans pursuant to sub-section 1 shall be updated within three months of completion of a sectoral risk and vulnerability assessment, cf. Section 99.

Section 101 At least every two years, the Danish Energy Agency shall hold emergency exercises for the oil, district heating and district cooling sectors, respectively, based on the sectoral preparedness plans pursuant to Section 100.

Section 102 The Danish Energy Agency shall prepare a plan of sectoral exercises which the Danish Energy Agency plans to implement for the oil, district heating and district cooling sectors over a five-year period. The plan shall be shared with impacted enterprises. (2) The five-year exercise plan for sectoral preparedness covers exercise elements in Annex 4 which the Energy Agency considers relevant for the oil, district heating and the district cooling sector.

(3) The five-year exercise plan for sectoral preparedness will be prepared for the first time to cover the period from 1 April 2025 to 31 March 2030. A new exercise plan is then prepared for a new five-year period.

Section 103 The Danish Energy Agency shall prepare an evaluation of the sectoral preparedness exercises within three months after a sectoral preparedness exercise has been held.

(2) The Danish Energy Agency shall share the conclusions from a sectoral preparedness exercise to enterprises in the oil, district heating and district cooling sectors.

Chapter 15

Privacy, exchange of information and digital communications

Section 104 Confidential information, cf. Section 26 of the Act on Enhanced Preparedness in the Energy Sector, shall be stored, handled and processed in a manner that ensures confidentiality, integrity and accessibility.

(2) Access to confidential information may only be granted to persons for whom such access is officially necessary or who can make legal requirements.

(3) Confidential information in physical and digital document form should be clearly marked as confidential.
(4) Documents referred to in sub-section 3 and portable digital storage media which have been used to store confidential information which are no longer used shall be destroyed or disposed securely in accordance with the confidentiality of the material, unless otherwise provided by law or provisions specified by law.

(5) Where the confidentiality and integrity of confidential information is detected or suspected, an assessment shall be made of whether such information being compromised is likely to pose a threat to the operation of the enterprise or the energy supply at the local, regional, national or European level. For confidential information in enterprises, this assessment is made by the enterprise, which shall notify the Danish Energy Agency without undue delay. Other confidential information is assessed by the Danish Energy Agency.

(6) The Danish Energy Agency may require enterprises to take mitigating measures in the event of incidents, cf. sub-section 5.

Section 105 Written communication from enterprises to the Danish Energy Agency on matters covered by the Act on Enhanced Preparedness in the Energy Sector and this Executive Order shall be made digitally through the designated self-service solution.

(2) The written communication referred to in sub-section 1 shall be understood as the sending and receipt of all relevant communications, documents and other communications as required by the provisions of the Act on Enhanced Preparedness in the Energy Sector or this Executive Order.

(3) Sub-section 1 shall not apply to enterprises which are exempted from compulsory access to Digital Post pursuant to the Executive Order exempting legal entities with a CVR number as well as natural persons with commercial activities for access to Digital Post.

(4) The digital communication shall use the public digital signature MitID Erhverv.

Section 106 The digital communication provided with the digital signature pursuant to Section 105(4) shall be deemed to have been delivered at the time when it is available to the Danish Energy Agency.

(2) The digital communication provided with the digital signature pursuant to Section 105(4) shall be deemed to have been sent by the specified sender.

(3) Written communications from enterprises to the Danish Energy Agency concerning matters covered by Section 105(1) shall not be deemed as received by the Danish Energy Authority if the enterprise has submitted the written communication in a manner other than as described in Section 105.

(4) In special cases, the Danish Energy Agency may process a written communication received in a manner other than as described in Section 105.

(5) In special cases, the Danish Energy Agency may process a written communication received digitally in accordance with Section 105 even if it is not provided with a digital signature as described in Section 105(4).

Chapter 16

Supervision and approval by the Danish Energy Agency of the enterprise's emergency response plan basis

Section 107 The Danish Energy Agency shall approve the conclusions of the enterprises on risk and vulnerability assessment, cf. Section 18, and contingency plans, cf. Section 19. Emergency response plans may be used during the approval process.

(2) Enterprises at levels 4 and 5 shall each year on 1 October send conclusions on an updated risk and vulnerability assessment, cf. Section 18, and updated emergency response plans, cf. Section 19, to the Danish Energy Agency - however for 2025, this deadline is 7 September.

(3) Enterprises in Level 2 and Level 3 shall every third year on 1 October send conclusions on an updated risk and vulnerability assessment, cf. Section 18, and updated emergency response plans, cf. Section 19, to the Danish Energy Agency. Enterprises in the district heating and district cooling sector shall send these conclusions for the first time on 1 October 2025. Enterprises in the gas, hydrogen and oil sectors respectively shall send these conclusions for the first time on 1 October 2026. Enterprises in the electricity sector shall these conclusions for the first time on 1 October 2027.

(4) Enterprises in Level 1 shall submit their emergency response plans, cf. Section 19(1-5), to the Danish Energy Agency at the request of the Danish Energy Agency.

(5) The Danish Energy Agency shall prepare risk and vulnerability scenarios which shall be included in the risk and vulnerability assessment of enterprises, cf. Section 18. Risk and vulnerability scenarios shall be

shared with undertakings no later than six months before enterprises are required to submit conclusions on an updated risk and vulnerability assessment to the Energy Agency pursuant to sub-sections 2-4.

(6) The Danish Energy Agency may require enterprises to update their risk and vulnerability assessment when the threat picture changes. Enterprises shall send an updated risk and vulnerability assessment to the Danish Energy Agency without undue delay.

Section 108 The Danish Energy Agency's supervision of enterprises shall be conducted on a frequency basis as specified in sub-sections 2-4.

(2) For enterprises at levels 4 and 5, supervision is carried out annually.

(3) For enterprises at level 3, supervision is carried out every three years.

(4) For enterprises at level 2, supervision is carried out every six years.

Section 109 The Danish Energy Agency's supervision is carried out using spot checks that are assessed to reflect an enterprise's overall compliance with the rules to a reasonable extent.

(2) The Danish Energy Agency's supervision can be carried out in other ways if the Danish Energy Agency deems that a more in-depth supervision is necessary.

(3) The Danish Energy Agency may base parts of the supervision on the audit of an enterprise to the extent that the Danish Energy Agency considers that the audit covers the matters being supervised.

Section 110 The Danish Energy Agency shall notify enterprises in writing about the completion of a physical inspection no later than 21 days before the inspection is to take place.

Section 111 The Danish Energy Agency may require enterprises to translate material to Danish when this material is to be used for the Danish Energy Agency's supervision. The cost of such translations shall be borne by the enterprise itself.

Section 112 The Danish Energy Agency shall prepare a report on the basis of the supervision that has been carried out. The report shall be submitted to enterprises for comment before completion.

(2) Enterprises may send a response to the report within two weeks of the report being submitted to them pursuant to sub-section 1.

(3) Enterprises shall, as soon as possible after completion of the supervision, submit the Danish Energy Agency's supervisory report to the management body of the enterprise with a view towards the management processing the Danish Energy Agency's conclusions.

Chapter 17

Coordinated preparedness

Section 113 Enterprises may apply in writing to establish coordinated emergency preparedness which entails that the emergency preparedness work pursuant to the Act on Enhanced Preparedness in the Energy Sector, the Executive Order on security approvals in the energy sector and this Executive Order is carried out jointly or by one party.

(2) Applications for coordinated preparedness shall be sent to the Danish Energy Agency for approval and shall contain at least the following:

1) A justification for the application.

2) A description of the geographical relationship between the enterprises.

3) A description of the organisational conditions of the enterprises and their differences.

4) A description of the advantages and disadvantages of the practical and technical impacts of coordinated preparedness.

5) How the operational efforts of the enterprises are to be managed, including the specification of the responsibilities and competencies of the enterprises as well as communication and information conditions.

(3) Energinet shall be consulted in the case of applications for coordinated preparedness for enterprises in the electricity, gas and hydrogen sectors respectively.

(4) When making its decision, the Danish Energy Agency places emphasis on whether a coordination of the preparedness of the enterprises should be considered to enhance the resilience and preparedness of each individual enterprise, the enterprises as a group and the energy sector as a whole.

Chapter 18

Identification of special enterprises

Section 114 The Danish Energy Agency shall identify and prepare a list of essential and important entities.

(2) The Danish Energy Agency shall carry out the tasks referred to in sub-section 1 for the first time by 17 April 2025 at the latest and then, where relevant, at least every two years.

(3) The Danish Energy Agency shall identify enterprises as significant enterprises in accordance with sub-section 1 if they meet one of the following conditions:

1) Enterprises exceeding one of the following thresholds:

a) Employs more than 250 people.

b) Has an annual turnover of over EUR 50 million and an annual total balance sheet of over EUR 43 million.

2) The enterprise is a critical enterprise pursuant to Section 115.

3) The enterprise is the sole provider in a member state for a service essential to the maintenance of critical societal or economic activities.

4) A disruption of the service provided by the enterprise could have a significant impact on public safety or public health.

5) A disruption of the service provided by the enterprise could result in a significant systemic risk, in particular for sectors where such disruption could have a cross-border effect.

6) The enterprise is critical because of its specific importance at the national or regional level for the sector or type of service in question or for other interdependent sectors in the member state.

(4) The Danish Energy Agency shall identify enterprises as important entities in accordance with sub-section 1 if they do not meet the criteria for being significant entities in accordance with sub-section 3 and if they meet at least one of the following conditions:

1) the entity employs more than 50 persons, or

2) the entity has an annual turnover of more than EUR 10 million and an annual total balance sheet of more than EUR 10 million.

Section 115 The Danish Energy Agency shall identify critical entities and prepare a list of these.

(2) The Danish Energy Agency shall carry out the tasks referred to in sub-section 1 for the first time by 17 July 2026 and subsequently, when relevant, however, at least every four years.

(3) Enterprises classified as Level 2-5 pursuant to Section 4 are critical entities.

(4) Enterprises shall be notified that they have been identified as a critical entity within one month after the Danish Energy Agency has drawn up the list referred to in sub-section 1.

(5) The Danish Energy Agency, when identifying enterprises pursuant to sub-section 1, shall duly take into account the results of Denmark's national risk assessment and national strategy for the resilience of critical entities prepared in accordance with the CER Directive, while also emphasising whether:

1) The enterprise provides one or more significant services.

2) The enterprise operates in and has its critical infrastructure located on Danish territory.

3) An incident at the enterprise will have a significant disruptive effect, cf. sub-section 6, on the enterprise's delivery of one or more essential services or on the delivery of other essential services in the sectors listed in Annex 5 which are dependent on this or these essential services.

(6) In determining whether an incident will have a significant disruptive effect as referred to sub-section 5, no. 3, the following shall be emphasised:

1) Number of users dependent on the significant service offered by the affected entity.

2) The extent of other sectors and subsectors dependency on the essential service in question.

3) The impact of incidents in terms of scale and duration on economic and societal activities, the environment, public safety or public health.

4) The market share of the entity in the market for the impacted essential services.

5) The geographical area that may be affected by an incident, including potential cross-border effects.

6) The importance of the entity in maintaining an adequate level of essential service, taking into account the availability of alternative means of delivering this essential service.

Section 116 The Danish Energy Agency shall identify critical entities of particular European importance.

(2) Enterprises that have received a notification pursuant to Section 115(4) shall, if they provide the same or similar essential services to or in six or more EU member states, inform the Danish Energy Agency of:

1) what essential services are provided, and

2) in which EU member states these essential services are provided.

(3) The Danish Energy Agency shall be notified pursuant to sub-section 2 as soon as possible and no later than one month after the notification pursuant to section 115(4).

(4) The Danish Energy Agency shall inform the European Commission as soon as possible of notifications received pursuant to sub-section 2.

(5) If the Danish Energy Agency receives a notification from the European Commission that the European Commission has concluded that the enterprise is a critical entity of particular European importance, the Danish Energy Agency shall inform the company about this, cf.

Section 5(2), of the Act on Enhanced Preparedness in the Energy Sector.

(6) Enterprises identified as a critical entity of particular European importance shall, upon completion of a advisory mission, cf. Section 20(1) of the Act on Enhanced Preparedness in the Energy Sector, report in writing to the Danish Energy Agency which of the measures the advisory mission has proposed that the enterprise carry out have been carried out by the enterprise.

(7) The Danish Energy Agency shall receive the report referred to in sub-section 6 no later than six months after the advisory mission has sent its statement with proposed measures to the enterprise identified as a critical entity of particular European importance.

Chapter 19

Dispensation

Section 117 The Danish Energy Agency may, upon application, derogate from the provisions of this Executive Order when the applicant has demonstrated that a derogation from the specific provision has a less significant or reduced effect on organisational preparedness, physical security and cybersecurity of the enterprise or the energy sector.

Chapter 20

Enforcement and avenues of complaint

Section 118 Decisions taken pursuant to the Act on Enhanced Preparedness in the Energy Sector and this Executive Order cannot be appealed to another administrative authority.

(2) However, decisions pursuant to sub-section 1 may be appealed to the Danish Energy Agency if it concerns legal questions.

Section 119 The Danish Energy Agency shall specify the areas in which the audit is to be carried out and specify the deadline for the completion of the audit in order to order the audit of an enterprise pursuant to Section 22(1) of the Act on Enhanced Preparedness in the Energy Sector.

Section 120 Audits pursuant to Section 119 shall be carried out by an independent auditor. The auditor shall be chosen by the enterprise itself and shall meet at least the following requirements:

1) The auditor may not have performed any tasks for the enterprise or intra-group enterprises in the last five full calendar years.

2) The auditor shall possess professional qualifications related to the area that is to be audited.

(2) The Danish Energy Agency shall approve the selected audit firm and the specific auditors to carry out the audit before the audit can be started.

(3) The enterprise shall, within two weeks of receipt of the order pursuant to Section 22(1) of the Act on Enhanced Preparedness in the Energy Sector, send information on the selection of the auditor, the price of the task and proof that the criteria in sub-section 1 have been met to the Danish Energy Agency. If the enterprise does not comply with the deadline, the Danish Energy Agency selects an auditor.

(4) The Danish Energy Agency has two weeks from the date of receipt of the request under sub-section 3 to approve or reject the choice of an auditor. If the Danish Energy Agency does not comply with the deadline, the audit can be started without approval.

Section 121 After the audit has been completed, the auditor's report shall be submitted to the Danish Energy Agency and the enterprise as soon as possible so that the Danish Energy Agency can make a decision as soon as possible on orders pursuant to Section 22(2) of the Act on Enhanced Preparedness in the Energy Sector.

Section 122 Unless a higher penalty is prescribed by other legislation, a fine shall be imposed on any entity which

1) violates Section 7, Section 10, Section 11(1-6 and 7), Sections 12-22, Section 23(1 & 2), Sections 24-76, Section 77(1 & 2), Section 77(4-7), Section 78(1), Section 79(1 & 2), Section 80, Section 104, Section 107(2-4), Section 112(3), Section 116(3, 6 and 7) and Section 120(1 & 3),

2) reports false, misleading information or fails to disclose information pursuant to Section 9(1, 2 and 3), Section 11(7), Sections 75-76, Section 77(3) and Section 78(1).

(2) Penalties imposed pursuant to sub-section 1 shall comply with the framework for determining the amount of the penalty in Section 37(1) of the Act on Enhanced Preparedness for the Energy Sector.

(3) Enterprises, etc. (legal persons) may be held criminally liable according to the rules in Chapter 5 of the Danish Criminal Code.

Chapter 21

Entry into force and transitional provisions

Section 123 This Executive Order will enter into force on 7 August 2025.

(2) The following Executive Orders are repealed:

1) Executive Order no. 11 of 7 January 2011 on the identification and designation of European critical energy infrastructure and assessment of the need for better protection (the EPCIP Directive).

2) Executive Order no. 424 of 25 April 2018 on emergency preparedness for the oil sector.

3) Executive Order no. 821 of 14 August 2019 on emergency preparedness for the natural gas sector.

4) Executive Order no. 2646 of 28 December 2021 on emergency preparedness in the electricity sector.

5) Executive Order no. 2647 of 28 December 2021 on IT emergency preparedness for the electricity and natural gas sectors.

(3) Measures under Sections 36 and 37 shall be implemented by 1 March 2026 at the latest, however, cf. sub-section 5.

(4) Measures under Sections 38, 43, 48, 50 and 62 shall be implemented by 1 March 2027 at the latest, however, cf. sub-section 5.

(5) Sub-sections 3 and 4 shall not apply to enterprises which have been subject to the provisions of Executive Order no. 424 of 25 April 2018 on emergency preparedness for the oil sector, Executive Order no. 821 of 14 August 2019 on emergency preparedness for the natural gas sector, Executive Order no. 2646 of 28 December

2021 on emergency preparedness for the electricity sector and Executive Order no. 2647 of 28 December 2021 on IT emergency preparedness for the electricity and natural gas sectors where the measures referred to in sub-sections 3 and 4 are substantially equivalent to those in the aforementioned Executive Orders.

Danish Energy Agency, 6 August 2025

Kristoffer Böttzauw

/ Jesper Rode Tholstrup

Annex 1

Forms with threshold values for level division of enterprises, cf. Section 4.

1. Thresholds for enterprises in the electricity sector

1.1. Thresholds for level 5

a) Electricity producers, designated electricity market operators and market participants providing services relating to aggregation, flexible electricity consumption or energy storage and which produce or manage a capacity of at least 1,650 MW of electricity production or consumption. Market participants providing services relating to aggregation, flexible electricity use or energy storage are included if they have the ability to control electricity production, electricity consumption or exchange electricity with the collective grid.

b) Operators of charging points responsible for the management and operation of a charging point providing a charging service to end users, including in the name of and on behalf of a mobility service provider and having a total capacity of at least 1,650 MW of electricity consumption from the collective grid.

c) Operators working with hydrogen production with a capacity of at least 1,650 MW of electricity from the collective grid.

d) Distribution system operators who manage a supply area with a minimum of 750,000 end-users or who in the last full calendar year have distributed a minimum of 3,500 GWh of electricity.

e) Transmission system operators.

f) Enterprises that have delegated authority tasks of importance for the electricity supply at the national level.

1.2. Thresholds for level 4

a) Electricity producers, designated electricity market operators and market participants providing services relating to aggregation, flexible electricity consumption or energy storage and producing or handling a capacity of at least 600 MW of electricity production or consumption. Market participants who provide services relating to aggregation, flexible electricity consumption or energy storage are included if they have the ability to control electricity production, electricity consumption or exchange electricity with the collective grid.

b) Operators of charging points responsible for the management and operation of a charging point providing a charging service to end-users, including in the name of and on behalf of a mobility service provider, and having a total capacity of at least 600 MW of electricity consumption from the collective grid.

c) Operators working with hydrogen production with a capacity of at least 600 MW of electricity consumption from the collective grid.

d) Distribution system operators who manage a supply area with a minimum of 250,000 end-users or who in the last full calendar year have distributed a minimum of 1,200 GWh of electricity.

e) Regional coordination centres.

1.3. Thresholds for level 3

a) Electricity producers, designated electricity market operators and market participants providing services relating to aggregation, flexible electricity consumption or energy storage and producing or handling a capacity of at least 100 MW of electricity production or consumption. Market participants who provide services relating to aggregation, flexible electricity consumption or energy storage are included if they have the ability to control electricity production, electricity consumption or exchange electricity with the collective grid.

b) Operators of charging points responsible for the management and operation of a charging point providing a charging service to end-users, including in the name of and on behalf of a mobility service provider, and having a total capacity of at least 100 MW of electricity consumption from the collective grid.

c) Operators working with hydrogen production with a capacity of at least 100 MW of electricity consumption from the collective grid.

d) Distribution system operators who manage a supply area with a minimum of 30,000 end-users or who in the last full calendar year have distributed a minimum of 150 GWh of electricity.

1.4. Thresholds for level 2

a) Electricity producers, designated electricity market operators and market participants providing services relating to aggregation, flexible electricity consumption or energy storage and which produce or manage a capacity of at least 25 MW of electricity production or consumption, provided that they have the ability to control electricity production, electricity consumption or exchange electricity with the collective grid, cf. point f.

b) Operators of charging points responsible for the management and operation of a charging point providing a charging service to end-users, including in the name of and on behalf of a mobility service provider, and having a total capacity of at least 25 MW of electricity consumption from the collective grid.

c) Operators working with hydrogen production with a capacity of at least 25 MW of electricity consumption from the collective grid.

d) Other distribution system operators managing a supply area and which are below the thresholds for levels 3-5.

e) Electricity companies that supply electricity and employ at least 50 employees or have an annual turnover of at least EUR 10 million and an annual total balance sheet of at least EUR 10 million.

f)	Market participants who provide services relating to aggregation, flexible electricity consumption or energy storage, but who only conduct transactions and do not have the ability to control electricity production, electricity consumption or exchange electricity with the collective grid are covered if they employ at least 50 employees or have an annual turnover of at least EUR 10 million and an annual balance sheet of at least EUR 10 million.
g)	Types of enterprises as referred to in points (a), (b), (c), (d), (e) and (f), employing at least 50 employees or having an annual turnover of at least EUR 10 million and an annual balance sheet of at least EUR 10 million.
1.5.	Thresholds for level 1 Not relevant

.	**Thresholds for enterprises in the gas sector**
2.1.	Thresholds for level 5
a)	Gas suppliers, LNG system operators, natural gas companies, natural gas refineries and processing plants operators and hydrogen storage operators that annually upgrade or inject at least 1,000 million Nm of ^{3} gas into a gas network or that annually produce or process at least 1,000 million Nm of ^{3} gas.
b)	Storage system operators having a total extraction capacity of at least 5 million Nm^3 gas per day or an injection capacity of at least 2 million Nm^3 gas per day.
c)	Enterprises that have delegated authority tasks of importance to the gas supply at the national level.
d)	Transmission system operators.
e)	Operators of upstream pipeline networks.
2.2.	Thresholds for level 4
a)	Gas suppliers, LNG system operators, natural gas companies, natural gas refineries and treatment plants operators and hydrogen storage operators that annually upgrade or inject at least 375 million Nm^3 of gas into a gas network or that annually produce or process at least 375 million Nm^3 of gas.
b)	Storage system operators having a total extraction capacity of at least 3 million Nm^3 gas per day or an injection capacity of at least 1 million Nm^3 gas per day.
c)	Distribution system operators and hydrogen transmission operators handling at least 100,000 Nm^3 gas per hour or managing a supply area with at least 250,000 end users

d)	City gas operators managing a supply area with a minimum of 250,000 end users
2.3.	Thresholds for level 3
a)	Gas supply enterprises, LNG system operators, natural gas enterprises, natural gas refineries and treatment plants operators and hydrogen storage operators that annually upgrade or inject at least 100 million Nm ^{3} of gas into a gas network or that annually produce or process at least 100 million Nm ^{3} of gas.
b)	Storage system operators having a total extraction capacity of at least 1 million Nm^3 gas per day or an injection capacity of at least 0.5 million Nm^3
c)	Distribution system operators and hydrogen transmission operators which handle a minimum of 10,000 Nm^3 gas/hour or which manage a supply area with a minimum of 30,000 end users
d)	City gas operators who manage a supply area with a minimum of 30,000 end users.
2.4.	Thresholds for level 2
a)	Gas suppliers, LNG system operators, natural gas enterprises, operators of natural gas refineries and treatment plants and hydrogen storage operators that annually upgrade or inject at least 26 million Nm^3 of gas into a gas network or that annually produce or process at least 26 million Nm^3 of gas.
b)	Storage system operators having a total extraction capacity of at least 0.5 million Nm^3 gas per day or an injection capacity of at least 200,000 Nm^3 gas per day.
c)	Other distribution system operators and hydrogen transmission operators.
d)	Other operators for city gas.
e)	The types of enterprises as referred to in points (a), (b), (c) and (d) employing at least 50 employees or having an annual turnover of at least EUR 10 million and an annual balance sheet of at least EUR 10 million.
2.5.	Thresholds for level 1
	Not relevant
3.	**Thresholds for enterprises in the oil sector**
3.1.	Thresholds for level 5
a)	Enterprises with delegated authority tasks.
b)	The central storage unit.

c) Operators of oil production plants, including offshore oil plants with an annual oil output of at least 1 million m^3 in three out of five years or with an expected oil output of at least 1 million m^3 in a calendar year.

d) Operators of oil refineries or oil treatment plants with an annual processing capacity of at least 1 million m^3 crude oil for three out of five years or with an expected processing capacity of at least 1 million m^3 crude oil for a calendar year.

3.2. Thresholds for level 4

a) Operators of oil transmission.

b) Operators of oil production plants, including offshore oil plants, with an annual oil production of at least 375,000 m^3 for three out of five years or with an expected oil production of at least 375,000 m^3 in a calendar year.

c) Operators of oil refineries or oil treatment plants with an annual processing of at least 375,000 m^3 of crude oil in three out of five years or with an expected processing of at least 375,000 m^3 of crude oil in a calendar year.

3.3. Thresholds for level 3

a) Operators of oil warehouses, including oil terminals with a total capacity of at least 300,000 m^3

b) Operators of oil production plants, including offshore oil plants, with an annual oil production of at least 100,000 m^3 for three out of five years or with an expected oil production of at least 100,000 m^3 for a calendar year.

c) Operators of oil refineries or oil treatment plants with an annual processing of at least 100,000 m^3 of crude oil for three out of five years or with an expected processing of at least 100,000 m3 of crude oil in a calendar year.

3.4. Thresholds for level 2

a) Operators of oil warehouses, including oil terminals with a total capacity of at least 100,000 m^3

b) Other enterprises with positive storage obligations.

c) Operators of oil production plants, including offshore oil plants, with an annual oil production of at least 26,000 m^3 for three out of five years or with an expected oil production of at least 26,000 m^3 in a calendar year.

d) Operators of oil refineries or oil treatment plants with an annual processing of at least 26,000 m^3 of crude oil in three out of five years or with an expected processing of at least 26,000 m^3 of crude oil in a calendar year.

e)	Operators of gas stations with a total annual sales of at least 600,000 m^3 or operating at least 100 gas stations in Denmark.
f)	The types of enterprises referred to in points (a), (b), (c) and (d) employing at least 50 employees or having an annual turnover of at least EUR 10 million and an annual balance sheet of at least EUR 10 million.
3.5.	Thresholds for level 1
	Not relevant

4. **Thresholds for enterprises in the district heating and district cooling sectors**	
4.1.	Thresholds for level 5
	Not relevant
4.2.	Thresholds for level 4
a)	Operators of district heating or district cooling that in two of the last three years have sold at least 4,525 GWh of district heating or district cooling.
4.3.	Thresholds for level 3
a)	Operators of district heating or district cooling that have sold at least 543 GWh of district heating or district cooling in two of the last three years.
4.4.	Thresholds for level 2
a)	Operators of district heating or district cooling that have sold at least 181 GWh of district heating or district cooling in two of the last three years.
b)	Local district heating or district cooling operators employing at least 50 employees or having an annual turnover of at least EUR 10 million and an annual balance sheet of at least EUR 10 million.
4.5.	Thresholds for level 1
a)	Operators of district heating or district cooling that in two of the last three years have sold at least 13.9 GWh of district heating or district cooling.

1. Thresholds for plants in the electricity sector	
1.1.	Thresholds for class 5
a)	Plants which are essential to maintain the supply of electricity to the interconnected electricity systems at the European level or substantial parts thereof.

b) Plants with capacity to produce at least 1,650 MW of electricity or consume at least 1,650 MW of electricity from the collective grid or which exchange at least 1,650 MW of electricity with the collective grid as well as plants that control these processes. This does not include distribution system operator's plants on the distribution network.

c) Hydrogen-producing plants with a capacity to consume at least 1,650 MW of electricity from the collective grid or reverse transfer at least 1,650 MW to the collective grid.

d) Plants of essential importance for the maintenance of the distribution of electricity to 750,000 end-users or for the distribution of 3,500 GWh of electricity.

1.2. Thresholds for class 4

a) Plants which are essential to maintain the supply of electricity to the interconnected electricity systems at the national level or substantial parts thereof.

b) Plants having the capacity to produce at least 600 MW of electricity or to consume at least 600 MW of electricity from the collective grid or to exchange at least 600 MW of electricity with the collective grid and plants controlling these processes. This does not include distribution system operator's plants on the distribution network.

c) Hydrogen-producing plants with a capacity to consume at least 600 MW of electricity from the collective grid or to reverse transfer at least 600 MW to the collective grid.

d) Plants of essential importance to maintain the distribution of electricity to at least 250,000 end users or for the distribution of at least 1,200 GWh of electricity.

1.3. Thresholds for class 3

a) Plants which are essential to maintain the supply of electricity to the interconnected electricity systems at the regional level or to substantial parts thereof.

b) Plants with capacity to produce at least 100 MW of electricity or to consume at least 100 MW of electricity from the collective grid or to exchange at least 100 MW of electricity with the collective grid and plants controlling these processes. This does not include distribution system operator's plants on the distribution network.

c) Hydrogen-producing plants with a capacity to consume at least 100 MW of electricity from the collective grid or to reverse transfer at least 100 MW to the collective grid.

d)	Plants of essential importance to maintain the distribution of electricity to 30,000 end users or the distribution of 150 GWh of electricity.
1.4.	Thresholds for class 2
a)	Plants capable of generating 25 MW of electricity or consuming 25 MW of electricity from the collective grid or exchanging 25 MW of electricity with the collective grid and plants controlling these processes. This does not include distribution system operator's plants on the distribution network.
b)	Hydrogen-producing plants with a capacity to consume 25 MW of electricity from the collective grid or reverse transfer 25 MW to the collective grid.
c)	Plants of essential importance for the maintenance of the distribution of electricity to 10,000 end users or for the distribution of 50 GWh of electricity.
1.5.	Thresholds for class 1
	Not relevant

. Thresholds for plants in the gas sector	
2.1.	Thresholds for class 5
a)	Plants essential to the maintenance of gas supply at the European level or substantial parts thereof.
b)	Plants that annually upgrade or inject 1,000 million Nm^3 of gas into the gas grid or that annually produce or process at least 1,000 million Nm^3 of gas.
c)	Gas storage facilities having a total extraction capacity of not less than 5 million Nm^3 gas per day or an injection capacity of not less than 3 million Nm^3 gas per day.
d)	Upstream pipeline networks.
2.2.	Thresholds for class 4
a)	Plants of essential importance to maintain the gas supply of the entire Danish gas supply system or substantial parts thereof.
b)	Plants that annually upgrade or inject at least 375 million Nm^3 of gas into a gas grid or which annually produce or process at least 375 million Nm^3 of gas.
c)	Gas storage facilities having a total extraction capacity of not less than 3 million Nm^3 gas per day or an injection capacity of not less than 1 million Nm^3 gas per day.
d)	Plants essential to maintain the distribution of 100,000 Nm^3 of gas per hour or for the distribution of gas to at least 250,000 end users.
e)	Plants essential to maintain the production or transportation of city gas to at least 250,000 end users.

2.3.	Thresholds for class 3
a)	Plants essential to maintain gas supply at the regional level or substantial parts thereof.
b)	Plants that annually upgrade or inject 100 million Nm^3 of gas into a gas grid or which annually produce or process at least 100 million Nm^3 of gas.
c)	Gas storage facilities having a total extraction capacity of not less than 1 million Nm^3 of gas per day or an injection capacity of not less than 0.5 million Nm^3.
d)	Plants essential to maintain the distribution of 10,000 Nm^3 of gas per hour or for the distribution of gas to at least 30,000 end users.
e)	Plants which are essential to maintain the production or delivery of city gas to a minimum of 30,000 end users.
2.4.	Thresholds for class 2
a)	Plants that annually upgrade or inject 26 million Nm^3 of gas into a gas grid or which annually produce or process at least 26 million Nm^3 of gas.
b)	Gas storage facilities having a total extraction capacity of at least 0.5 million Nm^3 gas per day or an injection capacity of at least 200,000 Nm^3 gas per day.
c)	Gas storage facilities having a total extraction capacity of at least 0.5 million Nm^3 gas per day or an injection capacity of at least 200,000 Nm^3 gas per day.
d)	Plants which are essential to maintain the production or delivery of city gas to at least 10,000 end users.
2.5.	Thresholds for class 1
	Not relevant

3. Thresholds for plants in the oil sector	
3.1.	Thresholds for class 5
a)	Plants of importance for the oil supply at the European level.
b)	Oil production plants and offshore oil plants with an annual production of at least 1 million m^3 in three out of five years or with an expected production of at least 1 million m^3 in a calendar year.
c)	Oil refineries and oil treatment plants with an annual processing of at least 1 million m^3 of crude oil in three out of five years or with an expected processing of at least 1 million m^3 of crude oil in a calendar year.
3.2.	Thresholds for class 4
a)	Oil pipelines and oil transmission plants with importance for the oil supply at the national level.
b)	Oil refineries of importance to the national oil supply.

c) Oil production plants and offshore oil plants with a minimum annual production of oil of 375,000 m^3 in three out of five years or with an expected oil production of at least 375,000 m^3 in a calendar year.

d) Oil refineries and oil treatment plants with a minimum annual processing of 375,000 m^3 of crude oil for three out of five years or with a expected crude oil processing of at least 375,000 m^3 in a calendar year.

3.3. Thresholds for class 3

a) Oil terminals or warehouses with a total capacity of at least 300,000 m^3.

b) Oil production plants and offshore oil plants with a minimum annual production of oil 100,000 m^3 in three out of five years or with an expected oil production of at least 100,000 m^3 in a calendar year.

c) Oil refineries and oil treatment plants with a minimum annual processing of 100,000 m^3 of crude oil for three out of five years or with a expected processing of at least 100,000 m^3 of crude oil in a calendar year.

3.4. Thresholds for class 2

a) Oil terminals and warehouses with a total capacity of at least 100,000 m^3.

b) Oil production plants and offshore oil plants with a minimum annual production of oil 26,000 m^3 in three out of five years or with an expected oil production of at least 26,000 m^3 in a calendar year.

c) Oil refineries and oil treatment plants with an annual processing of at least 26,000 m^3 of crude oil for three out of five years or with an expected processing of crude oil at least 26,000 m^3 in a calendar year.

3.5. Thresholds for class 1

Not relevant

4. Thresholds for plants in the district heating and district cooling sectors

4.1.	Thresholds for class 5 Not relevant
4.2.	Thresholds for class 4
a)	Plants essential to maintain the supply of at least 4,525 GWh of district heating or district cooling, including thermal power plants, district cooling plants, peak load and reserve plants, wiring networks, pump stations, heat exchanger stations, heat pumps and control rooms that control, regulate or monitor heat supplies.
4.3.	Thresholds for class 3
a)	Plants essential to maintain the supply of at least 543 GWh of district heating or district cooling, including thermal power plants, district cooling plants, peak load and reserve plants, wiring networks, pump stations, heat exchanger stations, heat pumps and control rooms that control, regulate or monitor heat supplies.
4.4.	Thresholds for class 2
a)	Plants essential to maintain the supply of at least 181 GWh of district heating or district cooling, including thermal power plants, district cooling plants, peak load and reserve plants, wiring networks, pump stations, heat exchanger stations, heat pumps and control rooms that control, regulate or monitor heat supplies.
4.5.	Thresholds for class 1 Not relevant

Annex 3

Information that enterprises shall submit to the Danish Energy Agency to allow the Danish Energy Agency's to make level categorisations of enterprises and the classification of plants, cf. Section 9.

1) Enterprise name, address and CVR number.

2) The relevant subsector to which the enterprise is subject, cf. Section 2 of the Act on Enhanced Preparedness in the Energy Sector.

3) Description of the service or services provided by the enterprise to the relevant subsector, cf. no. 2.

4) Updated enterprise contact information, including email addresses, IP intervals and telephone numbers.

5) Member states of the European Union where the enterprise provides services.

6) The enterprise's permit for energy production.

7) Information on the total amount of energy managed by the enterprise within a specified period, including:

a) The capacity of electricity that electricity producers, designated electricity market operators and market participants providing aggregation, flexible electricity consumption or power storage services can produce, consume or exchange with the collective grid.

b) The capacity of electricity that operators of charging points can manage or exchange with the collective grid. The information includes both the total power of the installed charging points and the available capacity for the overall portfolio of charging points.

c) The capacity of electricity that hydrogen production operators can consume from the collective electricity grid.

d) The amount of electricity distributed by distribution system operators in the last full calendar year.

e) The amount of gas that gas suppliers, LNG system operators, natural gas operators, natural gas refineries and treatment plants operators and hydrogen storage operators annually inject into or upgrade to a gas network or annually process or produce. The quantity shall be calculated in Nm3.

f) Extraction and injection capacity of storage system operators in Nm3 gas per day.

g) The amount of gas handled by distribution system operators and hydrogen transmission operators. The quantity shall be calculated in Nm3 gas per hour.

h) The capacity and the volume of gas transported which the operator of the upstream pipeline network can handle and which the enterprise has sold or otherwise handled during the last full calendar year.

i) The amount of oil produced annually by operators of oil production plants, including offshore oil plants, over the past five years and the expected oil production in the current calendar year.

j) The total capacity of oil storage facilities, including oil terminals, owned by oil storage operators.

k) The amount of oil processed annually by operators of oil refineries and oil treatment plants over the past five years and the expected oil processing in the current calendar year.

l) The capacity and transported quantity of oil which the oil transmission operator can handle and which the enterprise has sold or otherwise handled in the last full calendar year.

m) The total quantity of oil products sold by operators of gas stations in the last calendar year. The quantity shall be calculated in m3. In addition, operators of gas stations shall disclose the total number of gas stations owned by them.

n) The amount of heat and cooling sold annually by district heating and district cooling operators over the past three calendar years.

8) Information on the number of end users supplied by the enterprise, including:

a) Number of end users in the distribution system operator’s area of supply

b) The number of end users to which city gas operators deliver city gas.

9) Information on the enterprise's plants pursuant to no. 10-15, including the number of plants, type of plant, geographical location of the plant and the total amount of energy that the plant can handle or has handled within a specified period of time.

10) Production plants, plants with system-bearing properties, power distribution and transmission stations and connections in the electricity system that handle energy amounts corresponding to the threshold values for plants in the electricity sector, cf. Form 1 in Annex 2, including power plants, emergency start plants, transformers, cable transitions, station plants, cable plants, air-connection plants, wiring lines, reverse transfer plants, interconnection lines, wind turbines (including sea turbines), solar cells, batteries and hydrogen-producing plants.

11) Gas facilities handling energy amounts according to the threshold values for gas facilities, cf. Form 2 in Annex 2, including compressor stations, gas storage facilities, protection facilities, stations (M/R stations, reverse transfer facilities, line ventilation stations, pipelines), pipelines (transmission lines), upstream pipeline networks, natural gas refineries and treatment plants, gas production plants, upgrade plants, LNG facilities and control rooms that control, regulate or monitor the supply of gas.

12) Hydrogen-producing plants that consume or exchange electricity equivalent to the threshold values for plants in the electricity sector, cf. Form 1 in Annex 2, and hydrogen storage and transmission plants that handle quantities equivalent to the threshold values for plants in the gas sector, cf. Form 2 in Annex 2.

13) Oil sector plants handling energy volumes at the thresholds for oil sector plants, cf. Form 3 in Annex 2, including oil production plants, oil refineries, oil treatment plants, oil warehouses, oil terminals and oil transmission plants, including oil pipelines.

14) Number of plants in the district heating and district cooling sector that handle energy amounts corresponding to the threshold values for installations in the district heating sector, cf. Form 4 in Annex 2, including thermal power plants, district cooling plants, peak load and reserve plants, wiring networks, pump stations, heat exchanger stations, heat pumps and control rooms.

15) Control rooms which control, regulate or monitor deliverables to an energy system corresponding to the threshold values set out in Annexes 1 and 2.

16) Information on the enterprise's turnover, balance sheet and number of employees in the last two completed calendar years. The following information is requested for the last two completed calendar years:

a) Whether the enterprise had a minimum turnover of 10 million EUR.

b) Whether the enterprise had a minimum turnover of 50 million EUR.

c) Whether the enterprise had a balance sheet of at least 10 million EUR.

d) Whether the enterprise had a balance sheet of at least 50 million EUR.

e) Whether the enterprise had a minimum of 50 employees.

f) Whether the enterprise had a minimum of 250 employees.

Annex 4

Exercise elements, cf. Section 20

1. The enterprise's crisis management organisation.
. Securing of continued operations.
3. Restoration of supply.
4. Mobilisation of additional resources and materials.
5. Internal communication.
6. External communication.
7. Information for consumers.
8. The use of alternative communication channels.
9. Receipt and acknowledgement of notifications of changes in sectoral preparedness levels and sectoral preparedness measures.
10. Implementation of sectoral preparedness measures according to the sectoral preparedness level.
11. Receiving and handling alerts about cyber threats and vulnerabilities.
12. Procedures for coordinated preparedness.
13. Involving suppliers in handling incidents.
14. Involving suppliers of supply-critical network and information systems in handling incidents.
15. Activation of the enterprise's IT security service.
16. Emergency procedure for isolating supply-critical network and information systems in the production environment.
17. Emergency procedure for alternative operation of network and information systems and activation of redundant systems.
18. Recovery of supply-critical network and information systems from backups, including restoration of source code and system data for in-house-developed or specially developed software.
19. Normalisation after emergency operation of network and information systems.

Annex 5

Sectors of particular critical importance

Sector	Subsector	Type of entity
1. Energy	a) Electricity	– Electricity enterprises as defined in Article 2, no. 57) of Directive (EU) 2019/944[1] of the European Parliament and of the Council[(1)], which manage 'delivery' as defined in Article 2, no. 12) of that Directive.
		– Distribution system operators as defined in Article 2, no. 29), in Directive (EU) 2019/944.
		– transmission system operators as defined in Article 2 no. 35), in Directive (EU) 2019/944.
		– Producers as defined in Article 2, no. 38) of Directive (EU) 2019/944.
		– Designated electricity market operators as defined in Article 2, on. 8) of Regulation (EU) 2019/943[2)] of the European Parliament and of the Council[2)] – Market participants as defined in Article 2, no. 25) of the Regulation (EU) 2019/943 providing services relating to aggregation, flexible electricity consumption or energy storage as defined in Article 2, no. 18), 20) and 59), in Directive (EU) 2019/944. – Operators of charging stations responsible for the management and operation of a charging station providing a charging service to end users, including in the name of and on behalf of a mobility service provider.
	b) District heating and district cooling	– Operators of district heating or district cooling as defined in Article 2, no. 19) of Directive (EU) 2018/2001[3)] of the European Parliament and of the Council.
	c) Oil	– Oil pipeline operators.
		– Operators of oil production plants, refineries and treatment plants, oil storage and oil transport.
		– Central storage units as defined in Article 2(f) of Directive 2009/119/EC[(4)].
	d) Gas	– Supplier enterprises as defined in Article 2, no. 8) in Directive 2009/73/EC of the European Parliament and of the Council[5)].
		– distribution system operators as defined in Article 2, no. 6) Directive 2009/73/EC.
		– transmission system operators as defined in Article 2, no. 4) in Directive 2009/73/EC.
		– Storage system operators as defined in Article 2, no. 10) of Directive

		2009/73/EC.	
		– LNG system operators as defined in Article 2, no. 12) in Directive 2009/73/EC.	
		– Natural gas enterprises as defined in Article 2, no. 1) of Directive 2009/73/EC.	
		– Operators of natural gas refineries and treatment plants.	
	e) Hydrogen	– Operators in hydrogen production, storage and transmission.	
2. Transportation	a) Air	– Air carriers as defined in Article 3, no. 4) of Regulation (EC) No 300/2008 used for commercial purposes.	
			– Airport operators as defined in Article 2, no. 2) of Directive 2009/12/EC of the European Parliament and of the Council[6], airports as defined in Article 2, no. 1) of that Directive, including the main airports listed in Section 2 of Annex II for Regulation (EU) No 1315/2013[7] of the European Parliament and Council on entities with associated plants at airports.
			– Traffic management and control operators performing air traffic control functions as defined in Article 2, no. 1) of Regulation (EC) No 549/2004[8] of the European Parliament and of the Council.
		b) Railroads	– Infrastructure managers as defined in Article 3, no. 2) of the European Parliament and Council Directive 2012/34/EU[9].
			– Railway enterprises as defined in Article 3, no. 1) of Directive 2012/34/EU, including operators of service facilities as defined in that Directive's Article 3, no. 12).
		c) Water	– Shipping companies carrying out passenger and goods transportation by inland waterways, in high seas or coastal waters as defined for maritime transport in Annex I to Regulation (EC) No. 725/2004[10] of the European Parliament and Council except for individual vessels operated by these shipping companies.
			– Port operators as defined in Article 3, no. 1) of Directive 2005/65/EC of the European Parliament and of the Council[11], including their port facilities as defined in Article 2, no. 11) of Regulation (EC) No. 725/2004 and entities operating plants and equipment in ports.

			– Operators of maritime traffic services as defined in Article 3, point (o) in Directive 2002/59/EC of the European Parliament and of the Council[12].
		d) Road transport	– Road authorities as defined in Article 2, no. 12) of Commission Delegated Regulation (EU) 2015/962[13] responsible for traffic management, with the exception of public entities for which traffic management or operation of intelligent transport systems is a non-essential part of their general activity.
			– Operators of intelligent transport systems as defined in Article 4, no. 1) of Directive 2010/40/EU[14] of the European Parliament and of the Council.
3. Banking undertakings			Credit institutions as defined in Article 4, no. 1) of the European Parliament and Council Regulation (EU) No 575/2013[15].
4. Financial market infrastructures			– Operators of marketplaces as defined in Article 4, no. 24), in Directive 2014/65/EU of the European Parliament and of the Council[16].
			– central counterparties (CCPs) as defined in Article 2, no. 1) in Regulation (EU) No 648/2012[17] of the European Parliament and of the Council.
5. Health			– Healthcare providers as defined in Article 3(g) of European Directive 2011/24/EU of the European Parliament and of the Council[18].
			– EU reference laboratories referred to in Article 15 in Regulation (EU) 2022/2371[19] of the European Parliament and of the Council.
			– Entities carrying out research and development activities concerning medicinal products as defined in Article 1, no. 2) of the European Parliament and Council Directive 2001/83/EC[20]. – Entities manufacturing pharmaceutical raw materials and pharmaceutical compounds as referred to in Main Section C, Main Group 21, of NACE rev. 2. – Entities manufacturing medical devices which are considered to be critical in a public health crisis situation ('list of critical medical devices for public health crisis situations') as defined in Article 22 of Regulation (EU) 2022/123[21]

6. Drinking water			Suppliers and distributors of drinking water as defined in Article 2, no. 1), point (a) of Directive (EU) 2020/2184[22)] except for distributors for whom distribution of drinking water is a non-essential part of their general activity of distribution of other raw materials and goods.
7. Waste water			Enterprises collecting, disposing of or treating urban wastewater, household wastewater or industrial wastewater as defined in Article 2, no. 1), (2) and (3) of Council Directive 91/271/EEC[23)], except for enterprises for which the collection, disposal or treatment of municipal wastewater, household wastewater or industrial wastewater is a non-essential part of their general activity.
8. Digital infrastructure			– Providers of internet exchange points.
			– DNS service providers, other than operators of root name servers.
			– Top domain name administrators.
			– Providers of cloud computing services.
			– Providers of data centre services.
			– Providers of content delivery networks.
			– Validation service providers.
			– Providers of public electronic communications networks.
			– Providers of publicly available electronic communications services.
9. Management of ICT services (business-to-business)			– Providers of managed services. – Providers of managed security services.
10. Public administration			– Public administrative units under the central administration as defined by a member state in accordance with national law.
			– Public administrative units at the regional level as defined by a member state in accordance with national law.
11. Space			Operators of ground infrastructure owned, managed and operated by member states or private parties and supporting the provision of space-based services, excluding providers of public electronic communication networks.

(1) Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market in electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125).

(2) Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market in electricity (OJ L 158, 14.6.2019, p. 54).

(3) Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).

4) Council Directive 2009/119/EC of 14 September 2009 on the obligation of Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p. 9).

(5) Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 laying down common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

6) Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11).

(7) Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 laying down Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1).

8) Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 establishing the framework for the creation of a single European airspace ('the framework regulation') (OJ L 96, 31.3.2004, p. 1).

9) Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a common European railway area (OJ L 343, 14.12.2012, p. 32).

10) Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on improving the security of ships and port facilities (OJ L 129, 29.4.2004, p. 6).

11) Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on improving port security (OJ L 310, 25.11.2005, p. 28).

12) Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community traffic monitoring and traffic information system for maritime transport and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).

13) Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council as regards the provision of EU-wide real-time traffic information services (OJ L 157, 23.6.2015, p. 21).

14) Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on a framework for the introduction of intelligent transport systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

15) Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on supervisory requirements for credit institutions and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

16) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

17) Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade registers (OJ L 201, 27.7.2012, p. 1).

18) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on patient rights in relation to cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

19) Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border health threats and repealing Decision No 1082/2013/EU (OJ L 314, 6.12.2022, p. 26).

20) Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 establishing a Community code for medicinal products for human use (OJ L 311, 28.11.2001, p. 67).

21) Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 strengthening the role of the European Medicines Agency in crisis preparedness and crisis management in the field of medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1).

22) Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of drinking water (OJ L 435 of 23.12.2020, p. 1).

23) Council Directive 91/271/EEC of 21 May 1991 on the treatment of urban wastewater (OJ L 135, 30.5.1991, p. 40).