Ministry of Climate
and Environment

Risk-preparedness plan

Document prepared pursuant to Article 10 of Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC

Warsaw, 2021

Table of contents

List of tables and illustrations

List of legal acts

1. Act of 18 March 2010 on Specific Rights Vested to the Minister Responsible for State Assets and their Exercise in Certain Capital Companies or Capital Groups Operating in the Electricity, Oil and Gas Fuel Sectors (Journal of Laws of 2020, item 2173).
2. Regulation of the Prime Minister of 22 March 2017 on the Commissioner for Critical Infrastructure Protection (Journal of Laws of 2017, item 627).
3. Regulation of the Council of Ministers of 30 April 2010 on Critical Infrastructure Protection Plans (Journal of Laws of 2010, No. 83, item 542).
4. Regulation of the Council of Ministers of 31 October 2018 on the Thresholds for Considering an Incident as Serious (Journal of Laws of 2018, item 2180).
5. Act of 5 July 2018 on the National Cyber Security System (Journal of Laws of 2020, item 1369).
6. Act of 26 April 2007 on Crisis Management (Journal of Laws 2020, item 1856, and of 2021, item 159).
7. Act of 4 September 1997 on Government Administration Departments (Journal of Laws of 2020, item 1220 and 2327, and of 2021, item 255).
8. Act of 16 July 2004 on the Telecommunications Law (Journal of Laws of 2019, item 2460, and of 2020, item 374, 695 and 875).
9. Act of 10 June 2016 on Anti-Terrorist Activities (Journal of Laws of 2019, item 796).
10. Act of 6 June 1997 on the Penal Code (Journal of Laws of 2020, item 1444 and 1517).
11. Act of 10 April 1997 on the Energy Law (Journal of Laws of 2020, item 833, 843, 875, 1086, 1378 and 1565, and of 2021, item 234 and 255).
12. Regulation of the Council of Ministers of 23 July 2007 on the Detailed Principles and Procedures of Introducing Limitations on Sale of Solid Fuels and Supply and Consumption of Electricity or Heat (Journal of Laws of 2007, No. 133, item 924).
13. Regulation of the Council of Ministers of 15 December 2009 on Determining Government Administration Authorities that will Establish Crisis Management Centres and the Manner of their Operation (Journal of Laws of 2009, No. 226, item 1810).
14. Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC (OJ L 158, 14.6.2019, p. 1).
15. Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency (REMIT), (OJ L 326, 8.12.2011, p.1).
16. Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration (NC ER), (OJ L 312, 28.11.2017, p. 54, as amended).
17. Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation (SO GL), (OJ L 220, 25.8.2017, p. 1, as amended).
18. Regulation of the Council of Ministers on the Report on Threats to National Security (Journal of Laws of 2020, item 2344).

List of abbreviations

ABW	Internal Security Agency
CA	Competent authority as defined in Article 3 of Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC
CERT PSE	Computer Emergency Response Team operating at PSE S.A.
CI	Critical Infrastructure
CN	Supervision Centre - operating within the structure of PSE S.A.
CRP	cyber risk alert levels
CSIRT	Computer Security Incident Response Team
CZK	Crisis Management Centre
DSO	Distribution System Operator
DSR	Demand Side Response
EAS	ENTSO-E Awareness System - an IT tool used by the TSOs of ENTSO-E
ECG	European Commission's Electricity Coordination Group
EE–ISAC	European Energy – Information Sharing and Analysis Centre
EENS [%]	the value of expected undelivered energy volume (MWh) during the duration of energy supply constraints divided by the total value of annual electricity demand in the country (MWh)
EFTA	European Free Trade Association
ENTSO-E	European Network of Transmission System Operators for Electricity
FIRST	Forum of Incident Response and Security Teams
ICT	information and communication technologies
IRiESP	Instruction of Transmission System Operation and Maintenance
ISAC	Information Sharing and Analysis Centre
KDM	National Control Centre - operating within the structure of PSE S.A.
KPZK	National Crisis Management Plan
KSE	National Power System
LOLE [h]	the expected value of the number of hours during which the generating capacity does not meet demand in the power system due to a crisis scenario
MKiŚ	Ministry of Climate and Environment
MON	Ministry of National Defence
NASK	Research and Academic Computer Network - a national research institute for security and effective operation of ICT networks
NC ER	Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration
ODM	Regional Control Centre - operating within the structure of PSE S.A.
OT	Operational Technology

PSE	Polskie Sieci Elektroenergetyczne S.A.
PTPiREE	Polish Power Transmission and Distribution Association
RCB	Government Centre for Security
RCC	Regional Coordination Centre
RCN	Regional Supervision Centre - operating within the structure of PSE S.A.
REMIT	Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency
RSC	Regional Security Coordinator
SCO	low frequency demand disconnection
SGU	Significant Grid User
SOC	Security Operations Centre
SO GL	Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation
SOR	System Operation Region
SPO	Standard Operating Procedure
System EE	Electric power system
TGPE	Polish Power Plants Association
TSO	Transmission System Operator
WCZK	Voivodship Crisis Management Centre
ZIK	Critical Incident Team
ZZK	Crisis Management Team

General information

This document has been prepared pursuant to Article 10 of Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC and constitutes a risk-preparedness plan.

The purpose of developing this document is to avoid the occurrence or escalation of an electricity crisis and to mitigate its consequences. To ensure a common approach to the prevention and management of electricity crises, each Member State shall draw up such a plan based on pre-established regional and national electricity crisis scenarios. The risk-preparedness plans shall identify effective, proportionate, and non-discriminatory measures in relation to all identified electricity crisis scenarios, in particular national and regional measures that are necessary, especially in case of a simultaneous electricity crisis, i.e., affecting more than one Member State.

This document also defines the role and responsibilities of the competent authority designated pursuant to Article 3 of the above-mentioned Regulation (hereinafter referred to as the "competent authority" or "CA"), as well as the crisis coordinator as defined in Article 2 thereof. The competent authorities shall be responsible for performing the tasks provided for in this Regulation and shall cooperate with each other for the purpose of their implementation. The Minister responsible for energy (presently: Minister of Climate and Environment) has been designated as the competent authority for Poland.

The risk-preparedness plans will be updated on a regular basis. To ensure that the plans are up-to-date and effective, the competent authorities of the Member States of each region should organise, in cooperation with transmission system operators and other relevant stakeholders, electricity emergency simulations every two years to test their adequacy. It is envisaged that these may be carried out if the scope, approach, and timing of the simulations are agreed at regional level.

Name of the competent authority: Ministry of Climate and Environment.

Member States in the region: Poland belongs to the group of countries whose transmission system operators will be shareholders of the RCC for Central Europe SOR based in Munich (TSCNET). In addition to the Republic of Poland, the group includes: the Federal Republic of Germany, the Republic of Austria, the Czech Republic, the Republic of Slovenia, the Republic of Croatia, Hungary, the Slovak Republic, the Kingdom of the Netherlands, and Romania. The member states directly connected to Poland but not belonging to the same region are Sweden and Lithuania.

1. Summary of the electricity crisis scenarios

Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC ("Regulation 2019/941", OJ L 158, 14.6.2019, p. 1), required Member States to define and assess regional electricity crisis scenarios and identify national scenarios that form part of a risk-preparedness plan.

On 7 September 2020, ENTSO-E submitted to the entities indicated in Regulation 2019/941, including the Minister of Climate (presently Minister of Climate and Environment), a report summarizing the results of the identification and assessment of the most relevant regional electricity crisis scenarios. The work on the identification and assessment of the above-mentioned scenarios on the national side was carried out by the Polish transmission system operator, Polskie Sieci Elektroenergetyczne S.A., with the support of the Ministry of Climate and Environment.

Finally, ENTSO-E developed and submitted 31 regional electricity crisis scenarios that can be classified into the following categories: cyberattack, physical attack, extreme weather conditions, natural disasters, fuel supply, employee behaviour, market rules, technical errors, others. The list of scenarios developed by ENTSO-E, along with the characteristic identification number and category name, can be found in Table 1 below.

Table 1. Regional electricity crisis scenarios by category.

ID number	**Category**	**Scenario name**
1	Cyberattack	Cyberattack - entities connected to electrical grid
2		Cyberattack – entities not connected to electrical grid
3	Physical attack	Physical attack - critical assets
4		Physical attack – control centres
5		Threat to key employees
6		Insider attack
7	Extreme weather conditions	Solar storm
9		Storm
10		Cold spell
11		Precipitation and flooding
12		Winter incident
16		Multiple failures caused by extreme weather
28		Heatwave
29		Dry period
8	Natural disasters	Volcanic eruption
30		Earthquake
31		Forrest fire
27		Pandemic
13	Fuel supply	Fossil fuel shortage
14		Nuclear fuel shortage

20	Employee behaviour	Human error
23		Strike, riots, industrial action
25	Market rules	Unforeseen interaction of energy market rules
21		Unwanted power flows
15	Technical errors	Local technical failure
17		Loss of ICT systems for real-time operation
18		Simultaneous multiple failures
22		Serial equipment failure
19	Others	Power system control mechanism complexity
24		Industrial / nuclear accident
26		Unusually big RES forecast errors

Out of 31 scenarios provided by ENTSO-E, 3 scenarios have been considered by the expert assessment method as insignificant (including impossible) under Polish conditions and thus not requiring detailed analysis. These are:

- [14] Nuclear fuel shortage,
    - Poland does not have power generating modules operating on nuclear fuel.
- [8] Volcanic eruption,
    - Poland's location in Europe and large distances from active volcanoes (the distance between Poland and e.g., the active volcano in Iceland is over 2 thousand km, similarly in the case of volcanoes in Italy) mean that the eruptions themselves are not directly noticeable in Poland. Poland may be affected mainly by small fractions of ash (in the form of volcanic ash clouds), which does not seem to pose a threat to the operation of the system EE in Poland (neither in the form of a failure of its components nor in the form of a significant reduction of the power available in the system due to a decrease in PV generation at present and within the next 5 years).
- [30] Earthquake.
    - The territory of Poland in terms of seismic phenomena can be classified as an aseismic and penseismic area, where earthquakes occur quite rarely. Additionally, these are not strong quakes (up to 4.8 on the Richter scale). No earthquake with a magnitude greater than 4.8 on the Richter scale has been recorded in Poland over the last 100 years (it is pointed out that quakes with a magnitude of up to 4.8 are harmless, all known damages were possible only with a magnitude of 6.2 or more).

Other regional scenarios have been analysed and evaluated in detail. As part of the assessment, in case of scenarios considered relevant under Polish conditions, the regional perspective has been translated into national conditions. The evaluation of regional scenarios,

provided by ENTSO-E, was conducted in accordance with the Methodology to Identify Regional Electricity Crisis Scenarios[1].

Pursuant to Article 7 of Regulation 2019/941, based on regional electricity crisis scenarios, national electricity crisis scenarios have been identified after a consultation process.

The purpose of the consultation was to gather comments that could be used during the preparation of a national risk-preparedness plan, as well as to gather information related to the national dimension of regional electricity crisis scenarios. Forty-seven entities have been invited to the consultation and 33 of them responded, including: 6 DSOs (100% invited), 14 owners of power generating modules (100%), 11 demand facilities (73%), two representatives of institutions/associations (17%; RCB and TGPE).

The results of the consultation confirmed, from a national perspective, the relevance and appropriateness of the majority of the regional electricity crisis scenarios. The analysis did not identify proposals for additional scenarios that could serve as a basis for defining specific scenarios of a national electricity crisis. Therefore, the 28 regional electricity crisis scenarios described in the table above have been considered as national electricity crisis scenarios. Three regional electricity crisis scenarios have not been considered as national electricity crisis scenarios, as they are classified as insignificant to Polish conditions ([14] Nuclear fuel shortage, [8] Volcanic eruption, [30] Earthquake).

[1] Methodology to Identify Regional Electricity Crisis Scenarios pursuant to Article 5 of the Regulation of the European Parliament and of the Council on risk preparedness in the electricity sector and repealing Directive 2005/89/EC.

2. Roles and responsibilities of the competent authority

If there is specific, serious and reliable information from the seasonal adequacy assessment or other competent source that an electricity crisis may occur, the Competent Authority (CA) shall provide an early warning without delay to the relevant national authorities (including the RCB), the European Commission (EC), the competent authorities of the Member States located in the same region and, where they are not located in the same region, the competent authorities of the directly connected Member States.

The CA shall also provide information on the causes of a possible electricity crisis, the measures planned or undertaken to prevent an electricity crisis and the possible need for assistance from other Member States.

In the face of an electricity crisis, the CA, after consultation with the Polish transmission system operator, shall declare an electricity crisis and without undue delay inform the competent authorities of the Member States in the same region and, if they are not in the same region, the competent authorities of the directly connected Member States and the EC. This information shall include the reasons for the deterioration of the electricity supply situation, the reasons for declaring an electricity crisis, the measures planned or undertaken to mitigate the crisis and if there is a need for assistance from other Member States.

After the CA issues an early warning or declares an electricity crisis, the measures specified in the risk-preparedness plan shall be implemented to the maximum extent possible.

A detailed scheme of action in the event of an energy crisis is included in the Risk Management Plan of the Minister of Climate and Environment and in the KPZK. The tasks regarding the prevention and preparation phase concerning disturbances in the electricity system, indicated for implementation by the minister responsible for energy (CA) are:

1. the preparation of a draft state electricity policy and coordination of its implementation,
2. the determination, by way of a regulation, of detailed conditions for the operation of the electricity system, taking into account security and reliable operation of this system, construction and operation of equipment, installations, and grids,
3. the supervision of key service operators,
4. monitoring the functioning of the National Power System and security of electricity supply.

The tasks of each minister (head of a central office) carried out in a crisis situation include:

1. Monitoring, coordinating, and directing activities, especially:
    a) monitoring the situation and providing information on a regular basis, taking into account the procedures in place for the exchange of information,
    b) confirming the principles of cooperation with interested entities,
    c) the process of activating tasks and coordinating activities, and in the case of a cooperating entity, taking into account the support resulting from the demand of other entities,
    d) convening a meeting of the Minister's Crisis Management Team,
    e) requesting the convening of a Government Crisis Management Team.
2. Mobilization of external resources.

3. Actions in the event of an imminent threat or unavailability of office personnel, facilities, or equipment:
    a) action in the event of an alert level or CRP alert level,
    b) activation of a warning and emergency alert system for the office's own personnel,
    c) maintaining the ability to manage a crisis situation in the event of damage to or unavailability of facilities and infrastructure anticipated for the operation of the Minister's Crisis Management Team,
    d) activation of the process of restoring the operational readiness of its own institution as well as subordinate, supervised, or dependent organizational structures.
4. Launching the process of social communication, including:
    a) organization of actions against disinformation.

Tasks of the minister responsible for energy (the competent authority) include:

1. Intervention activities with respect to:
    a) the sale of solid fuels,
    b) the supply and consumption of electricity,
2. Intervention activities on the natural gas market.
3. Intervention activities on the crude oil and liquid fuels market.
4. The provision of strategic reserves and the creation of reserves outside the Government Strategic Reserve Programme.
5. Supporting activities to restore and ensure continuity of operation of critical infrastructure under the minister's responsibility.

The purpose of identifying priorities for critical infrastructure protection and restoration is to mitigate and reduce the natural and anthropogenic effects of disruptions to its functioning, including those transmitted to other facilities, installations, equipment, and services that make up critical infrastructure systems (cascading effects), and to restore the functions it performs as quickly as possible.

Given that all facilities, installations, equipment, and services that form the infrastructure systems are important for the functioning of the State and the satisfaction of citizens' needs, critical infrastructure (CI) protection priorities, in accordance with the principle of equity identified in the National Critical Infrastructure Protection Programme, shall be set at an equal level.

In the event of an emergency, priorities for protecting and restoring critical infrastructure can change dynamically as the emergency unfolds and are dependent on many factors.

The most important include:

1. The type of risk and the nature of its spread.
2. The scale of the risk.
3. The number of citizens affected by the disruption of services provided by the CI.
4. The affected area.

The Minister of State Assets in the critical infrastructure protection system acts as a coordinator of the energy, energy raw materials and fuels supply system, together with the Minister of Climate and Environment. The system of supply of energy, energy raw materials and

fuels includes companies operating in the electricity sector - having infrastructure for either generation or transmission of electricity.

The Minister of State Assets, as the only one of the ministers responsible for critical infrastructure systems, has specific powers to supervise the coordinated system. If irregularities are found, the Minister of State Assets, after consultation with the Minister of Climate and Environment, may object to resolutions passed by company bodies or legal acts carried out by company management that pose a real risk to the operation, continuity of operations and integrity of critical infrastructure[2]. In accordance with the provisions of the Law and the Regulation of the Prime Minister of 22 March 2017 on the Commissioner for Critical Infrastructure Protection (Journal of Laws of 2017, item 627), the Minister of State Assets, in consultation with the Director of the Government Centre for Security, approves the appointment and dismissal of the Commissioner for Critical Infrastructure Protection in companies operating in the electricity, oil and gas fuels sectors, whose property is included in the unified list of facilities, installations, equipment and services constituting critical infrastructure. The Commissioner for Critical Infrastructure Protection is an employee of the company who monitors the company's critical infrastructure protection activities and is responsible for maintaining contact with relevant entities.

Pursuant to the Regulation of the Council of Ministers of 30 April 2010 on Critical Infrastructure Protection Plans (Journal of Laws of 2010, No. 83, item 542), the Minister of State Assets approves critical infrastructure protection plans developed by critical infrastructure operators of the energy, energy resources and fuels supply system and the communications system.

As part of the monitoring of the State's energy security, the Ministry of State Assets participates in the meetings of the Electricity Risk Monitoring Team.

By Order of the Minister of Climate dated 26 March 2020, the Team for ensuring national energy security has been established. The tasks of the Team include planning, initiating, and coordinating activities to ensure the energy security of the State, as well as initiating and coordinating countermeasures and interventions when this security is endangered. It consists of representatives of: Minister of Climate and Environment, Minister of State Assets, Director of the Government Centre for Security, President of the Energy Regulatory Office (National Regulatory Authority), President of the Government Strategic Reserve Agency, Head of the Internal Security Agency, and Government Plenipotentiary for Strategic Energy Infrastructure.

In addition, to ensure the effectiveness of crisis management tasks (prevention, preparedness, response, recovery, including restoration of the CI resources), a Crisis Management Centre has been established at the Ministry of Climate and Environment, which is on 24-hour duty seven days a week including public holidays.

The essence of the above organization of work is to ensure continuous monitoring of the departments of government administration subordinate to the Minister of Climate and Environment (energy, climate, and environment) and optimal flow of information both between individual heads of organizational units as well as between them and cooperating entities - in particular RCB, WCZK, uniformed services.

Monitoring of the Minister of Climate and Environment's Risk Management Centre is carried out based on a systematic and unified reporting system. This system, in addition to determining the present state, also includes elements of forecasts and estimation of potential risks in individual sectors. The adopted procedure for evaluation of reports allows the person on duty in

[2] The powers of the Minister of State Assets with respect to critical infrastructure are set out in the Act of 18 March 2010 on Specific Rights Vested to the Minister Responsible for State Assets and their Exercise in Certain Capital Companies or Capital Groups Operating in the Electricity, Oil and Gas Fuel Sectors (Journal of Laws of 2020, item 2173).

the Crisis Management Centre to take appropriate alert decisions. Access to the reports of individual managers of organizational units allows for free flow of information within the structure.

At the same time, it should be mentioned that in the Ministry of Climate and Environment there is a Crisis Management Team (ZZK) established for the decision-making by the Minister, which includes all directors of the organizational units of the Ministry. The responsibilities of this Team include ensuring the implementation of the Minister's tasks in terms of monitoring risks to state security, including information on the readiness to provide services by the country's electricity sectors, the state of material reserve resources, waste management, the state of risks in the area of cybersecurity, environment, as well as developing proposals for the Minister on actions to prevent and counter these risks, in the situation of an epidemic state due to Covid-19 virus infections.

The system described above proved itself many times in the face of critical situations. An example can be its functioning (together with a specially established Team) during the ongoing Covid-19 virus pandemic.

In order to strengthen the monitoring process and increase energy security was established the Team for ensuring national energy security. The main goal of the works of this Team is to provide the Minister of Climate and Environment, as the state body responsible for ensuring energy security, with support in the execution of his tasks in this area by entities to which the law grants competences in the field of energy security. The scope of the Team's activities enables the collection of complete information, on the current situation in energy systems, essential for the Minister of Climate and Environment to make decisions preventing the occurrence of possible disruptions in the functioning of these systems or their effects.

3. Procedures and measures in the electricity crisis

3.1. National procedures and measures

3.1.1. Procedures to be followed in the cases of an electricity crisis, including the correspondence schemes on information flows.

3.1.1.1. Procedures used by the competent authority.

The detailed scheme of action in case of an electricity crisis is contained in the Minister of Climate and Environment's Crisis Management Plan and the National Crisis Management Plan. The method of communication developed on their basis shall be implemented according to the points below:

1. The Competent Authority (CA) is responsible for monitoring risks that could lead to an electricity crisis.
2. The flow of information on risks resulting from monitoring and on the occurring events is ensured by the CA Crisis Management Centre (CZK CA) with the support of other organisational units of the CA.
3. In the case of receiving, as the first one, information about the risk, the CA immediately notifies the Director of the RCB as well as higher and lower-level authorities, respectively, and the transmission system operator. In the procedure, this information has the form of an ad hoc report. It contains information that can be determined immediately after the occurrence of the event, as of a certain hour, in particular:
   a) the type of event or risk (if the risk is described in the crisis management plan, the name of the risk used in this plan should be given),
   b) the description of the situation or the type of event or risk, including the causes as well as the time and place or area (voivodship, county, municipality, town) of its occurrence,
   c) the actual and potential consequences of an event or risk,
   d) the assessment and forecast of a development of the situation,
   e) the description of actions taken and intended to be taken,
   f) the description of the forces and resources committed and expected to be deployed,
   g) conclusions and recommendations or comments,
   h) the source of information about the event or risk.

Communication is accomplished through the use of available electronic and telephone means (verbal, written information).

4. In the event that information from an ad hoc report, monitoring data, or situation assessment indicates the possibility of, or confirms the occurrence of, a crisis situation, the CA shall report on the situation and the course of action in the form of a situation report. This report shall be submitted periodically, as requested by a higher-level authority, until the completion of actions related to a crisis situation. When situational reporting is activated, an ad hoc report shall not be made. The situation report shall contain information on the activities being conducted, as of a given day/hour, in accordance with letters (a)-(h) of point 3 above.

5. Irrespective of submitted ad hoc or situation reports, the CA prepares and submits, in the crisis management centre (CZK) system, periodically, once every 24 hours, information on the situation as well as on implemented and planned actions. This information has the form of a daily report. The report shall include:

   a) significant events and risks identified during the past 24 hours,

   b) identified potential risks (and their possible consequences),

   c) actions planned in relation to events/risks (if not included in the situation report),

   d) the adequacy of available forces and means to the conducted/planned actions.

Government Centre for Security (RCB), based on received daily reports, prepares daily summary information and forwards it to ministries, heads of central offices, voivodes.

The concept for reporting on crisis events and actions taken, as well as the conceptual scheme of the monitoring, warning and alerting system on risks are presented in the illustrations below. The detailed circulation of information between national authorities and structures of crisis management is included in SOP-12 of the KPZK, part B.

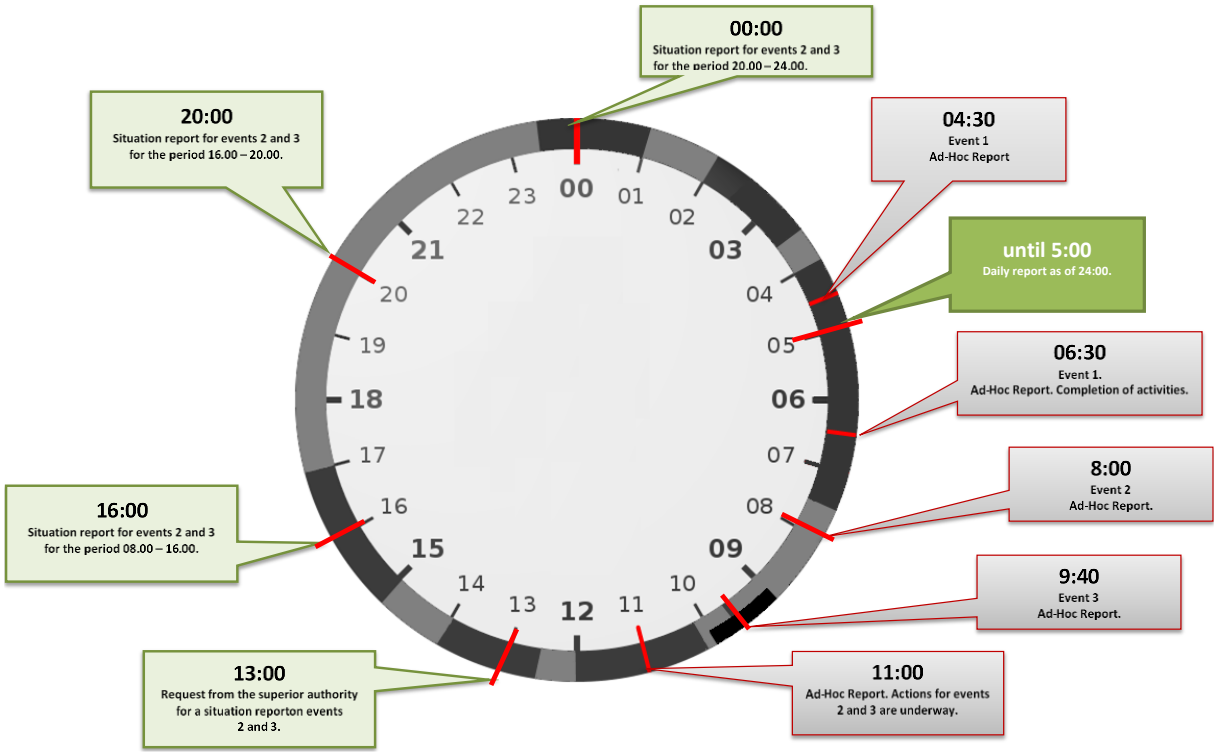

Illustration 1. Event and Action Reporting - a demonstration solution when three events occur in a 24-hour period (based on KPZK, Part B, p. 143).

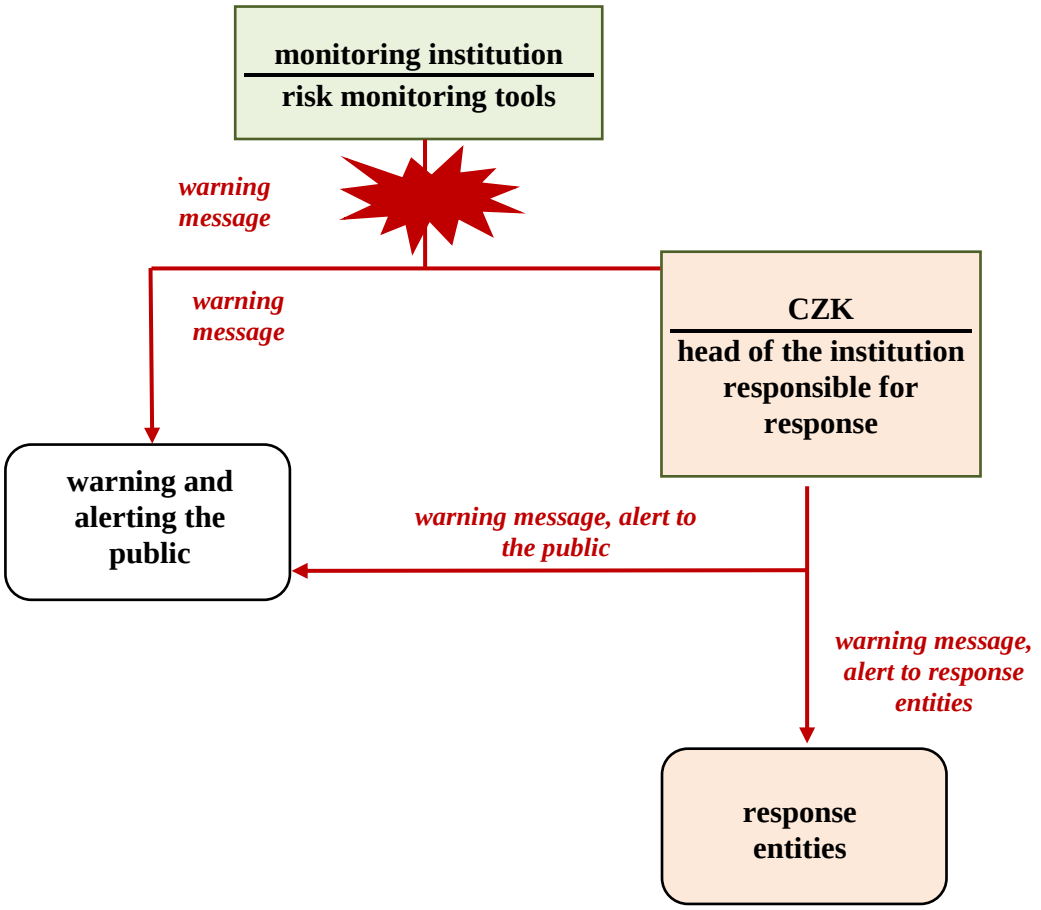

Illustration 2. Schematic diagram of the monitoring, alert, and warning system (as per: KPZK)

3.1.1.2.Information obligations of the Transmission System Operator

The information obligations of the Transmission System Operator (hereinafter also referred to as the "TSO" or "Operator") that are performed in the event of an electricity crisis include (but are not limited to):

1. Publishing information as part of fulfilling its obligations under Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency (hereinafter referred to as the "REMIT", OJ L 326, 8.12.2011, p.1).
2. Transmitting to the minister responsible for energy, on a daily basis, information on the operation of the National Power System (hereinafter referred to as the "KSE") during the previous day and the expected conditions on the current day. Such information shall include, inter alia, data on forecasted demand, available generation capacities and data on fuel stocks, as well as which data shall be obtained from generators.
3. Informing, via the TSO's website, about the occurrence of a state of risk to the security of electricity supply.

4. Informing the minister responsible for energy and the President of the Energy Regulatory Office in the event of a risk to the security of electricity supply.
5. Publishing information on the need to introduce restrictions on the supply and consumption of electricity through the TSO's website and Program I of the Polish Radio, previously submitting the applications and information required by law to the minister responsible for energy and the President of the Energy Regulatory Office.

3.1.1.3. Cyber-incidents

In case of risk of occurrence or occurrence of an electricity crisis caused by a cybersecurity incident (cyber-incident), the entity in which the incident occurred classifies the incident as serious based on the thresholds[3] for considering it as serious, and reports such incident immediately, but no later than within 24 hours of its detection, to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV. The role of relevant CSIRTs is to classify reported serious incidents as critical (if such incidents result in significant damage to security or public order, international interests, economic interests, operation of public institutions, civil rights and freedoms, or human life and health), and to coordinate handling of such incidents. The relevant national level CSIRTs shall communicate with each other about the critical incident, along with other required information, and provide information about this incident to the Government Centre for Security. This information shall also include a recommendation to convene a Government Crisis Management Team and may include a request to convene a Critical Incident Team.

In addition to the above, the procedures contained in the Crisis Management Plan of the entity where the incident occurred shall be followed, and the procedures contained in the National Crisis Management Plan shall be activated, in particular the one concerning the convening and handling of the Critical Incident Team meeting (see table on the following pages).

[3] The thresholds for considering an incident as serious are defined in the Regulation of the Council of Ministers of 31 October 2018 on the Thresholds for Considering an Incident as Serious (Journal of Laws 2018, item 2180).

Table 2. Convening and handling a meeting of the Critical Incident Team[4] (as per: KPZK)

I. Purpose of procedure, coordinator of activities, legal basis

Purpose of procedure	**Coordinator of activities**	**Participants**
Define the decision-making and organizational process for convening a meeting of the Critical Incident Team (hereafter referred to as the ZIK) in the event of a critical incident[5] in the area of cybersecurity of the Republic of Poland.	Director of Government Centre for Security	Permanent members of the team: - representatives of CSIRT MON, CSIRT NASK, CSIRT GOV (Head of ABW) Members invited to the team meeting, in particular, representatives of: – the Government Plenipotentiary for Cybersecurity, – the minister responsible for energy, – the minister responsible for transport, – the minister responsible for maritime economy, – the minister responsible for inland navigation, – the minister responsible for health matters, – the minister responsible for water management, – the minister responsible for informatization, – the minister responsible for internal affairs, – the Minister of National Defence, – the Minister of Justice,

[4] The scope and functioning of the Critical Incident Team is defined in Article 36 of the Act of 5 July 2018 on the National Cyber Security System (Journal of Laws of 2020, item 1369).

[5] Critical incident - an incident resulting in significant damage to security or public order, international interests, economic interests, operation of public institutions, civil rights and freedoms or human life and health, classified by the competent CSIRT MON, CSIRT NASK or CSIRT GOV.

			– the Minister of Foreign Affairs, – the Minister-Special Services Coordinator, – the National Public Prosecutor, – the Financial Supervision Commission (KNF), – the President of the Office of Electronic Communications, – the Commander-in-Chief of Police, – the Commander of the Central Investigation Bureau of the National Police Headquarters, – the Commander of the State Protection Service, – the Commander-in-Chief of the Polish Border Guard, – the Government Centre for Security, – other institutions (including a voivode competent territorially for the consequences of the event) based on a decision of the ZIK chairperson.
Input	Output	Legal basis for action	
Occurrence or high probability of occurrence of a critical incident in the area of cybersecurity of the Republic of Poland	Communicate the findings of the ZIK meeting to operators.	1) Act of 5 July 2018 on the National Cyber Security System (Journal of Laws of 2020, item 1369). 2) Act of 26 April 2007 on Crisis Management (Journal of Laws 2020, item 1856, and of 2021, item 159). 3) Act of 4 September 1997 on Government Administration Departments (Journal of Laws of 2020, item 1220 and 2327, and of 2021, item 255). 4) Act of 16 July 2004 on the Telecommunications Law (Journal of Laws of 2019, item 2460, and of 2020, item 374, 695 and 875). 5) Act of 10 June 2016 on Anti-Terrorist Activities (Journal of Laws of 2019, item 796).	

II. Course of actions

<table>
<tr><th>No.</th><th>Activity</th><th>Method of performing the task</th><th>Performer</th></tr>
<tr><td rowspan="2">1.</td><td rowspan="2">Collection of incident data and preparation of the situation information</td><td rowspan="2">The information shall include:
1) a preliminary analysis of the potential impact of the incident, including:
a) the number of users affected, especially if it disrupts critical services provided by those users,
b) when the incident has been occurred, detected, and how long it will last,
c) the geographic extent of the area affected,
2) a possible recommendation for convening a Government Crisis Management Team[6],
3) a possible request to convene the ZIK together with recommendations concerning the composition of the invited representatives and the secrecy of the meeting.</td><td>Head of CSIRT MON, CSIRT NASK, CSIRT GOV</td></tr>
<tr><td>The authority competent in matters of crisis management, pursuant to Article 21 of the Act on Crisis Management.</td></tr>
<tr><td>2.</td><td colspan="2">Provide the prepared information to the Director of the Government Centre for Security.</td><td>– head of CSIRT MON, CSIRT NASK, CSIRT GOV,
– the authority competent in matters of crisis management, pursuant to Article 21 of the Act on Crisis Management.</td></tr>
</table>

[6] The impact of the incident may be of such magnitude that a Government Crisis Management Team will be convened before a CSIRT information will be prepared and a proposal will be made to convene a ZIK to determine incident handling policies and identify a lead CSIRT.

3.	Preparation of a compiled summary information. Communication of the compiled summary information, along with a decision to convene the ZIK, as well as the date and place of the ZIK meeting to the team members scheduled to attend it.		Director of the RCB
4.	Preparation of the ZIK meeting place	1) preparation of briefing materials on the incident for meeting participants, its impacts (including secondary impacts and sector interdependencies), and projected course, 2) preparation of visualization of the operational situation and participation in the meeting via electronic communication means, 3) only as needed - preparation and protection of the meeting site as per the appropriate security classification[7], 4) ensuring that the meeting will be documented, 5) the meeting shall be chaired by the Director of the RCB.	Director of the RCB
5.	Findings (decisions) resulting from the ZIK meeting	1) the unanimous designation of a CSIRT to coordinate the handling of a critical incident, 2) defining tasks and roles of other CSIRTs and RCB in handling the incident, 3) determine how to exchange technical information regarding the incident,	Director of the RCB

[7] If it is not possible to hold a classified meeting on the RCB's premises, the meeting shall be held on the premises of the Ministry of the Interior and Administration or the Internal Security Agency.

		4) preparation of information policy recommendations resulting from the situation, 5) deciding on a possible application by the Director of the RCB to the Prime Minister on convening a Government Crisis Management Team, 6) in case of an incident that may pose a risk of a terrorist nature[8], concerning information and communication systems of public administration authorities or information and communication systems that constitute critical infrastructure[9], preparation of information and conclusions for the minister responsible for internal affairs and the Head of the Internal Security Agency[10].	
6.	Communication of the findings (decisions) made at the ZIK meeting to its participants for implementation		Director of the RCB

[8] An event of a terrorist nature should be understood as a situation which is suspected to have been caused by an offence of such a nature, as referred to in Article 115 § 20 of the Act of 6 June 1997 on the Penal Code, or a risk of such an offence.

[9] Act on Anti-Terrorist Activities "Art.15.2. In the case of a risk of a terrorist event concerning information and communication systems of public administration authorities or information and communication systems that constitute critical infrastructure, or in the case of the occurrence of such an event, one of the four CRP alert levels may be introduced:
1) CRP first alert level (ALFA-CRP level);
2) CRP second alert level (BRAVO-CRP level);
3) CRP third alert level (CHARLIE-CRP level);
4) CRP fourth alert level (DELTA-CRP level)".

[10] The Act on Anti-Terrorist Activities "Art. 16. 1. Alert levels or CRP alert levels shall be activated, changed and cancelled, by way of an ordinance, depending on the type of the risk of a terrorist event, by the Prime Minister, after consultation with the minister responsible for internal affairs and the Head of the Internal Security Agency, and in urgent cases - by the minister responsible for internal affairs, after consultation with the Head of the Internal Security Agency, immediately notifying the Prime Minister thereof:
1) on the entire territory of the Republic of Poland;
2) on the territory of one or more districts of the country;
3) on the territory defined other than by reference to the regional districts of the country;
4) for specific facilities of organizational units of public administration, prosecutor's office, courts or other facilities of infrastructure of public administration or critical infrastructure".

7.	Formal communication of the adopted findings (decisions) to the meeting participants		Director of the RCB
8.	Keeping the RCB informed about the situation and the status of implementation of the findings adopted at the ZIK meeting		– Head of CSIRT MON, CSIRT NASK, CSIRT GOV – the authority competent in matters of crisis management, pursuant to Article 21 of the Act on Crisis Management
9.	Monitoring the situation. Preparing periodical reports		Director of the RCB
10.	If there was such a ZIK decision - a request to the Prime Minister to convene a Government Crisis Management Team	Preparing and conducting the meeting of the Government Crisis Management Team	Director of the RCB

3.1.2. Preventive and preparatory measures

1. To ensure security of supply, the TSO undertakes a number of measures, some of which involve monitoring and planning of the operations of the National Power System (KSE). These include:

   a) Monitoring of system parameters in the long and short term within the scope of the planning of the grid operation, the purpose of which is, among other things, to maintain the N-1 security criterion.

   b) Activities undertaken as part of the market-based system balancing process.

   c) Maintaining the required levels of power reserves in the KSE.

   d) Security analysis performed online in dispatch support systems.

   e) Monitoring transmission grid elements when security levels are found to be compromised.

   f) Monitoring of weather forecasts with respect to the impact of weather conditions on the demand for electricity, generation, or transmission capacity, as well as with respect to the occurrence of extreme weather events. Data in this scope is obtained from official information services as well as on the basis of bilateral agreements concluded with specialized entities, e.g., data, exclusively for internal use of the TSO, intended for the forecast of generation from renewable energy sources.

   g) Monitoring of fuel stocks available for power generating modules (PGM).

2. To ensure a proper planning of the grid operation, information on a number of parameters of the operation of the power system shall be exchanged. It includes TSOs, Distribution System Operators, PGMs, and other relevant electricity market participants. The catalogue of information to be exchanged is defined in the document "Scope of data to be exchanged for the purpose of planning the operation and maintenance of the KSE", which was developed pursuant to Article 40(5) of Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation (SO GL, OJ L 220, 25.8.2017, p. 1, as amended) and approved by the National Regulatory Authority.

3. In addition, TSOs use or have at their disposal a number of measures that are aimed at preventing and preparing for situations that may have a significant negative impact on operation and security of supply. These include:

   a) Actions aimed at the maximum utilization of the generating capacities available in the KSE, including but not limited to the utilization of the full range of the available capacity of the generation modules, ordering the operation with overload for the power generating modules for which contracts for such service have been concluded, ordering start-up of the power generating modules.

   b) Changing the grid topology, it means changing the active/reactive power flows by changing the grid topology, i.e., changing tap position on transformer, phase shifters, switching off/on busbar couplers at substations, lines, capacitors , shunt reactors, respectively.

   c) Demand Side Response (DSR) at the request of the TSO.

   d) If necessary, announcing "at-risk period" during which there is a power obligation for PGMs participating in the power market.

4. To ensure secure functioning of the information systems important for correct operation of the KSE, the TSO shall carry out on-going monitoring of:

   a) The ICT processes.

   b) Information and communication security events (performed round-the-clock by the Security Operations Centre - SOC).

5. Moreover, at the stage of planning, implementation and operation of information systems and data communication network, to ensure the required level of their resilience to incidents and events, the TSO shall:

   a) Implement technical and organizational solutions based on the best security standards.

   b) Apply network segmentation and separation of assets with different sensitivities.

   c) Consider the need to ensure high availability, multi-level redundancy mechanisms and principles of secure operation. In this respect, applicable are:

      – voice communication systems with redundant equipment and emergency power sources, supported by public mobile and satellite telephony,

      – emergency (radio) dispatch communication systems with redundant equipment and power sources available only on about 25% of the country's area.

      – data transmission network with redundant equipment, operating in a reliability-performance system,

      – primary and backup data centres with redundant infrastructure, equipped with transmission and processing equipment, operating in a reliability-performance system,

      – ICT systems built in a way that ensures simultaneous work in two data processing centres and based on an architecture that allows minimizing data loss in case of a failure of the said centre.

6. The TSO shall cooperate with specialized government agencies and other entities included in the electricity sector for the exchange of experience and information in the area of cyber security.

   a) The Computer Emergency Response Team operating at the TSO (hereinafter referred to as the "CERT PSE") coordinates the work of the Cyber Security Team at the Ministry of Climate and Environment. The members of this Team are entities belonging to the electricity sector). The Team produces bulletins/reports addressed to all Team members, including information on:

      – IT and OT vulnerabilities published in a given period.

      – Helpful tools to use in the area of cybersecurity.

      – Statistical data on events and incidents that have occurred.

   b) CERT PSE works closely with CSIRT GOV, CSIRT NASK and CSIRT MON, receiving information from these entities regarding the latest cyber security risks and recommendations on how to mitigate them. CERT PSE also reports to the above-mentioned entities on the security measures implemented at the TSOs and concerning cyber security.

c) CERT PSE is connected to several risk monitoring systems and transmits information on Indicator of Compromise (IoC), showing the characteristics associated with a given incident.

d) Additionally, there are bilateral cooperation agreements in place between CERT PSE and CERTs/CSIRTs established in other electricity sector entities, which concern raising the level of cyber security in the sector, sharing knowledge about risks, and respond to them jointly.

7. Within the framework of building a national cyber security system, the TSO actively participates in legislative work and the development of security standards, both at the national and European level.

8. To ensure the physical security of facilities belonging to the TSO:

a) The following are developed, agreed, and maintained up to date: Critical Infrastructure Protection Plans, Plans for the protection of facilities subject to mandatory protection and Continuity of Operations Plan. Periodic tests of solutions provided for in the above-mentioned plans are carried out. In case of emergencies or alert levels referred to in the anti-terrorist act, TSO implements actions provided for in the a/m planning documents.

b) The TSO shall enter into and maintain multi-year contracts for the safeguarding of facilities that are part of the infrastructure managed directly by the TSO.

c) Technical means of physical security (mechanical and electronic) shall be used.

d) The TSO authorizes and controls the access to the above-mentioned facilities (specific access zones established therein) both for its own employees and for representatives of entities cooperating with it. Detailed rules of conduct have been defined in this respect. In case of shared facilities, appropriate agreements regulating the rules of access shall be concluded.

e) Enhanced physical security measures shall be applied to power dispatch centres (National Control Centre - KDM, Regional Control Centre - ODM) and supervision centres (Supervision Centre - CN, Regional Supervision Centre - RCN). They also concern the locations of backup control rooms and supervision centres maintained by TSOs.

9. The TSO has established and maintains a systematic approach to prevent and prepare for incidents of deliberate attacks against the Operator which may affect its ability to perform assigned tasks.

3.1.3. Mitigating measures

1. In the event of an emergency a Crisis Team is appointed in TSO, whose task is to monitor the situation on an ongoing basis and to prepare and coordinate a response appropriate to the changing conditions.

2. In case of a risk to the security of electricity supply in the KSE, the TSO, in cooperation with the system users, including electricity Customers, shall undertake any possible actions using available means aimed at removing such risk and preventing its negative consequences. Examples of measures at the disposal of the TSO are listed in the catalogue defined by national legislation. These include:

a) Issuing an order to the PGM to start up, shut down, change setpoint, or disconnect a centrally dispatched power generating module from the grid.

b) Making emergency purchases of active power.

c) Issuing an order to the appropriate Distribution System Operator to start up, shut down, change setpointd, or disconnect from the grid a PGM connected to the distribution grid within its area of operation that is not a centrally dispatched power generating module.

d) Issuing an order to the relevant Distribution System Operator to reduce the amount of electricity consumed by the end customers connected to the distribution grid in its area of operation or interrupting the supply to the necessary number of end customers connected to the distribution grid in that area.

e) Making reductions in the amount of interchange capacity.

f) Proclaiming "risk period" during which there is a capacity obligation for PGMs participating in the capacity market.

g) After exhaustion of all possible measures aimed at meeting the demand for electricity and only in order to counteract the threat to the security of electricity supply in the KSE, issuance to the end users, as defined in the Regulation of the Council of Ministers of 23 July 2007 on the Detailed Principles and Procedures of Introducing Limitations on Sale of Solid Fuels and Supply and Consumption of Electricity or Heat (Journal of Laws of 2007, No. 133, item 924, as amended), an order to reduce the amount of electricity taken in accordance with the "Plan for introducing restrictions in the supply and off-take of electricity" approved by the President of the Energy Regulatory Office (National Regulatory Authority).

3. It is assumed that the measures to be taken by the TSO in case of a risk to electricity supply should cause minimum disturbance to the operation of the electricity market, should be applied in the scope necessary to restore proper functioning of the electricity system and on the basis of the criteria adopted for the current balancing of the electricity system and system congestion management, and should be taken in agreement with the relevant operators of the electricity transmission systems, pursuant to the provisions of the agreements, in particular regarding the exchange of information.

4. The resources at the TSO's disposal referred to in point 2 above, shall be operationalized in the form of a number of measures. These include both the measures indicated in point 3 of subsection 3.1.2., which may also be applied to mitigate the electricity crisis, as well as, among others, the actions presented below:

a) Suspension and restoration of market operations - in accordance with the rules approved by the President of the Energy Regulatory Office and developed by the TSO pursuant to Article 36(1) and Article 39(1) of the NC ER.

b) Interconnection outages, if pre-emptive separation of the KSE for asynchronous operation is a condition for maintaining the integrity and security of the system operation.

c) Measures provided for under the System Defence Plan developed pursuant to Article 11 of the NC ER, including but not limited to, emergency limitations, low frequency demand disconnection (hereinafter referred to as the "SCO"), interconnection line

outages, use of the Significant Grid Users (SGU) capabilities in an alert and emergency system state .

d) Measures provided under the Restoration Plan developed pursuant to Article 23 of the NC ER, including, but not limited to, the use of SGU capacity in the blackout and restoration system states, KSE restoration instructions.

5. With respect to information systems and telecommunications network, which are important for the proper operation of the KSE, the TSO ensures ongoing incident handling and a structured approach to security incident response.

6. In cases where it is justified by the physical security of the transmission infrastructure or the TSO personnel, the rules for calling and cooperation with relevant uniformed services shall apply.

7. In the event of deterioration in the epidemic situation of the country and a significant increase of the risk level of mass illnesses among its own employees, TSO assumes:

a) the issuance of guidelines for the provision of work, the implementation of TSO tasks and cooperation with external entities in the emergency sanitary regime,

b) the introduction and maintenance of physical separation of critical teams in all locations to ensure the continuity and security of critical processes.

8. Procedures for cooperation, including sharing information about incidents or risks to the transmission infrastructure security:

a) The PSE S.A. Continuity of Operations Plan sets forth the rules for PSE S.A. cooperation with administrative authorities and public services concerning information in case of a serious disturbance in the transmission system, including the information and communication infrastructure. They provide for the transmission of information by the TSO to: Plenipotentiary for Strategic Energy Infrastructure, the minister responsible for energy, the Government Centre for Security and the Computer Security Incident Response Team led by the Head of the Internal Security Agency.

b) The Critical Infrastructure Protection Plans include catalogues of mutual information provided by TSOs and the following entities: local government authorities, voivodship administrative authorities, the minister responsible for energy, the Government Centre for Security, the Police, the State Fire Service, and the Internal Security Agency. This catalogue has been defined based on the obligations arising from the relevant provisions of law and the agreements concluded.

c) The TSO concludes and maintains agreements with selected Distribution System Operators and other entities with which it shares facilities or on whose territory such facilities are located. These agreements concern, among other things, the exchange of information about possible security risks to these facilities.

d) The TSO has defined and applies a number of detailed procedures/instructions for information exchange. These covers, inter alia, crisis situations, risk of terrorist attacks, suspicions of criminal acts, coordination of actions with respect to proceedings conducted by law enforcement authorities, computer security incidents.

3.1.4. Framework for the introduction of restrictions on customer power consumption

In the event of a threat to the security of electricity supply, including a long-term imbalance in the fuel and energy market in the whole or part of the country, restrictions on the supply and off-take of electricity may be imposed for a specific period of time[11]. This shall be done by way of a regulation of the Council of Ministers, upon the request of the minister responsible for energy (the competent authority). The motion shall be prepared by the minister responsible for energy on his/her own initiative or on the basis of notifications from the TSO (for electricity). Restrictions on the supply and off-take of electricity consist in limiting the maximum electric power and daily electricity consumption. These restrictions are subject to compliance control by the relevant state authorities, including the President of the Energy Regulatory Office. Pursuant to Polish law, electricity companies are not liable for the consequences of restrictions imposed in this manner.

The Minister responsible for energy shall immediately inform the European Commission, the Member States of the European Union, and the Member States of the European Free Trade Association (EFTA) about the introduced limitations as well as actions and measures taken to eliminate the state of risk to security of electricity supply.

The introduction of restrictions on the supply and off-take of electricity (in the "normal" mode - introduced by the Council of Ministers at the request of the minister responsible for energy or in the mode "by order of the TSO") is a measure that depends on the decision of the state authorities - it requires the action of the relevant authorities (Council of Ministers, minister responsible for energy). The mode of introducing restrictions on the supply and off-take of electricity "by order of the TSO" may be used only until the relevant regulations by the Council of Ministers will be issued and no longer than for 72 hours.

Restrictions on the supply and off-take of electricity are implemented by Distribution System Operators (DSOs) upon order of the TSO. Pursuant to statutory requirements, the Instruction of Transmission System Operation and Maintenance (IRiESP) contains the system congestion management procedures based on which the TSO orders DSOs to introduce restrictions. Detailed regulations in this respect are also set forth in the Regulation of the Council of Ministers of 23 July 2007 on the Detailed Principles and Procedures of Introducing Limitations on Sale of Solid Fuels and Supply and Consumption of Electricity or Heat (Journal of Laws of 2007, No. 133, item 924).

According to the provisions of the above-mentioned Regulation, limitations in the supply and off-take of electricity cannot be source of:

1. endanger the safety of people or damage or destroy technological facilities,
2. interference in the operation of facilities intended for the performance of tasks related to:
    a) national security or defence,
    b) healthcare,
    c) telecommunication,
    d) education,
    e) exploitation of fossil fuels from deposits, their processing and supply to consumers,
    f) generation and supply of electricity to customers,

[11] Regulations in this area are described, among others, in the Act of 10 April 1997 on the Energy Law (Journal of Laws of 2020, item 833, 843, 875, 1086, 1378 and 1565, and of 2021, item 234 and 255).

g) environmental protection.

According to this regulation, special protection covers:

1. electricity consumers throughout the year, for which the contracted power is set below 300 kW,
2. hospitals and other medical emergency facilities,
3. mass media facilities with national coverage,
4. airports,
5. international railroad facilities,
6. military, energy, and other facilities of strategic importance for the functioning of the economy or the state,
7. facilities that have technical measures to prevent or reduce emissions that adversely affect the environment.

When preparing plans to introduce restrictions in their areas, DSOs shall take into account the need to ensure electricity supply to facilities, taking into account the above-mentioned criteria.

3.1.5. Mechanisms used to inform the public about the electricity crisis.

3.1.5.1. Mechanisms used by the competent authority and the RCB.

1. The spokesperson/head of the organizational unit in charge of CA public communication is responsible for coordinating communication with the public through the media.
2. The Head of the CA shall ensure communication with the public in all other areas by designating individuals responsible for a particular area.
3. The spokesman/head of the organisational unit in charge of CA public communication may appoint a Crisis Press Team, consisting of representatives of the press units of the entities involved in solving the crisis situation. In the event that the Team does not present a unified position, the spokesperson of the CA has the casting vote. In the case of appointment of the Crisis Press Team, the Team, chaired by the CA spokesperson, determines the main messages, communication tools and appoints communicators.
4. To serve on the Crisis Press Team, experts may be invited.
5. If information coming out from the involved entities is not consistent or is false - the Government Centre for Security shall inform the appropriate spokespersons to ensure consistency of the message.
6. The RCB shall conduct communications with the public during a crisis within the scope of its authority. It assumes the role of primary communicator and lead entity in the aspect of public communication in a given crisis situation, if such arrangements are made at a meeting of the Government Crisis Management Team.
7. The Government Spokesperson may delegate the coordination of information policy to a spokesperson from an institution other than the CA.

3.1.5.2. Information duties of TSO

1. Public disclosure of information in fulfilment of obligations related to the implementation of REMIT.
2. Informing, via the TSO's website, about the occurrence of a risk to the security of electricity supply.

3. In case of the necessity to introduce restrictions on the supply and off-take of electricity, the TSO shall publish such information via its website and the Polish Radio Program I.

3.2. Regional and bilateral procedures and measures

3.2.1. Agreed mechanisms for cooperation within the region and for ensuring appropriate coordination before and during the electricity crisis, including the decision-making procedures for appropriate reaction at regional level.

1. There are currently no specific mechanisms or processes implemented by or involving the Regional Security Coordinator (RSC) that are applicable to an electricity crisis.
2. Inter-operator cooperation in the region is carried out on the basis of inter-operator agreements concluded between the TSO and transmission system operators of other countries. A distinction should be made between:
   a) bilateral agreements (e.g., "System Operating Agreement") that are concluded with transmission system operators of all neighbouring member state countries (the Federal Republic of Germany, the Czech Republic, the Slovak Republic), and
   b) regional agreement ("Synchronous Area Framework Agreement" - SAFA), which covers all the transmission system operators operating in the synchronous area of Continental Europe and defines the principles of operation of the synchronous system in the normal state as well as in emergency and restoration system state (e.g., "Policy on Emergency and Restoration"). SAFA fulfils the provisions of Article 13 of SO GL and Article 10 of NC ER.
3. The TSO is engaged in the exchange of experience and information in the area of cyber security.
   a) CERT PSE is a member of organisations associating security teams in Europe (Trusted Introducer) and worldwide (FIRST). A target of these organizations also includes cooperation and exchange of information on cyber security (information about new vulnerabilities, risks, and incidents).
   b) CERT PSE is also a member of EE-ISAC (European Energy ISAC), whose task is to share knowledge about risks.

3.2.2. Any regional and bilateral measures that have been agreed, including any necessary technical, legal and financial arrangements necessary for implementation of those measures.

1. Within the framework of inter-operator cooperation, carried out with the participation of regional transmission system operators:
   a) arrangements for the supply or sale of power and energy from abroad shall be made,
   b) measures provided within the framework of inter-operator agreements shall be applied after prior exhaustion of adequate national measures.
2. In terms of information exchange at the inter-operator level, there are (inter alia):
   a) arrangements for short- and long-term planning of the European electricity system,
   b) cooperation at the level of the European Network of Transmission System Operators for Electricity (ENTSO-E),

c) continuous monitoring of the current system status using the ENTSO-E Awareness System (EAS) tool.

3.2.3. Mechanisms in place for cooperation and for coordinating actions, before and during the electricity crisis, with other Member States outside of the region as well as with third countries within the relevant synchronous area.

1. Inter-operator cooperation with Member States from outside the region as well as with third countries within the synchronous area of Continental Europe is carried out, with the participation of the TSO, based on:

   a) Bilateral inter-operator agreements (e.g., "System Operating Agreement"), which are concluded with the transmission system operators from neighbouring countries (Ukraine, Lithuania, Sweden).

   b) Inter-operator agreements of a regional nature (e.g., "Synchronous Area Framework Agreement"), which cover all the transmission system operators operating in the synchronous area of Continental Europe and specify the principles of operation of the synchronously operating system in the normal state as well as in emergency and restoration system state (e.g., "Policy on Emergency and Restoration"). SAFA fulfils the provisions of Article 13 of SO GL and Article 10 of NC ER.

4. Crisis Coordinator

The Crisis Coordinator is the Minister of Climate and Environment. Acting as the competent authority responsible for ensuring security of electricity supply, he/she:

1. monitors and analyses the situation regarding security of electricity supply,
2. coordinates the activities of all entities in the event of a crisis situation,
3. submits an application to the Council of Ministers for the introduction of restrictions on electricity consumption - by way of a regulation on the whole or part of the country,
4. is responsible for communication with the European Commission (EC),
5. the representative of the Minister of Climate and Environment shall attend ECG meetings and ensure exchange of information between the European Commission and the Minister of Climate and Environment.

When faced with an emergency situation, the Minister of Climate and Environment has the ability to convene a Crisis Management Team (ZZK).

Note: When an electricity crisis is part of a larger crisis beyond the purview of the Minister, the Government Centre for Security shall take the lead role in information acquisition, analysis, and distribution.

Contact to the Crisis Coordinator via the MKiŚ Crisis Management Centre: zrk@klimat.gov.pl, phone: +48 22 36 92 354.

Contact to the 24/7 emergency service of the Government Centre for Security: dyzurny@rcb.gov.pl, phone: +48 22 361 69 00, +48 785 700 177.

5. Stakeholder consultations

In accordance with Article 10(1) of Regulation 2019/941, a competent authority of each Member State shall establish a risk-preparedness plan, after consulting TSOs and DSOs considered relevant by the competent authority, the transmission system operators, the relevant producers or their trade bodies, the electricity and natural gas undertakings, the relevant organisations that represent the interests of industrial and non-industrial electricity customers, and the regulatory authority where it is not the competent authority.

During the preparation of this document, a working team has been established, consisting of representatives of the competent authority, namely the Minister of Climate and Environment, represented by persons from substantive units for electricity and cyber security; the national TSO; the Ministry of State Assets; and the Government Centre for Security. All proposals as to the content and shape of the risk-preparedness plan were agreed upon in this forum. Actively participating in the working group, the mentioned entities prepared their contributions to the risk-preparedness plan. Additionally, input was also sought from representatives of Polish DSOs affiliated with the Polish Power Transmission and Distribution Association (PTPiREE).

In conducting the international consultation process with Member States in the region, directly connected Member States and the ECG, the Minister of Climate and Environment will concurrently circulate the risk-preparedness plan to national stakeholders for consultation, pursuant to Article 10(1) of Regulation 2019/941, while taking into account to the extent possible the comments received during the international consultation process.

6. Emergency tests

6.1. Testing the effectiveness of national procedures

In order to prepare for a possible electricity crisis, the competent authorities of the Member States of each region, with the participation of relevant stakeholders, shall periodically test the effectiveness of the national procedures developed in the risk-preparedness plans, including information-sharing and cooperation mechanisms.

The role of initiator in the organization of crisis response tests, at the national level, is held by the Minister of Climate and Environment. The response tests shall be held according to the established schedule, and their date and the entity responsible for their organization shall be designated by the Minister of Climate and Environment (competent authority). It is assumed that the scenario of the response test should be prepared in a narrow expert group and cannot be disclosed to test participants until the implementation of the test. The scenario should assume a sequence of events grading potential problems in the operation of the electricity system up to an event requiring the activation of response measures described in this plan, including up to the point where non-market measures will be necessary. It is also acceptable to assume a scenario that immediately leads to a significant disruption in the operation of the electricity system materializing with high EENS and LOLE ratios over a significant area, including the area of more than one Member State (the so-called "simultaneous electricity crisis").

As part of the scenario preparation, the main actors who should participate in the test (stakeholders) should be identified. The crisis response test scenario should assume variants of the test course depending on the decisions made by its participants.

The crisis response test scenario is subject to approval by the Minister of Climate and Environment, and the entities identified in the test (stakeholders) are obliged to participate. The tests should use the same mechanisms and means of communication as during a real crisis. In order not to confuse the test with the actual communication, the test messages should be properly marked. The implementation of the test should take place in conditions as close to real ones as possible. In the course of testing, evaluations or conclusions should be avoided. It is advisable to define the function of observers not involved in the tests in order to record events, decisions, procedures, and instructions used and to identify facts occurring during crisis response tests.

After the completion of the crisis response test, there should be a phase of summarizing the results obtained in its framework. A summary of the findings, a timeline of events and recommendations after the completion of the test, the entity responsible for the implementation of the test should present in the final report submitted to the Minister of Climate and Environment.

6.2. Regional simulations of real-time response to electricity crises

1. As of the date of this document, a schedule for regional electricity crisis simulations has not yet been developed and agreed.
2. The TSO participates in activities that are not currently part of such a schedule but serve to ensure preparedness in the event of an electricity crisis. These include:
   a) exercises conducted with participation of TSO and transmission system operators of neighbouring countries on a simulator of the European power system in case of emergency situations in this system,
   b) exercises conducted by the TSO with participation of Distribution System Operators on a KSE simulator in case of emergencies in the system,

c) national level tests carried out by TSOs, Distribution System Operators and generators, in accordance with the test plan approved by the President of the Energy Regulatory Office and developed under Article 43 (2) of the NC ER.