ENERGY REGULATORY AUTHORITY

DRAFT-Strategy for critical infrastructures in the power sector

This strategy shall be used in accordance with the "National Authority for Electronic Certification and Cyber Security"

Article 1

Authority

Energy Regulatory Authority based on article 18 of Law No. 43/2015 "On Power Sector", exercises its regulatory functions to promote an internal competitive market which shall be safe and friendly to the environment for all the customers and suppliers, ensuring the appropriate conditions for a safe and sustainable operation of the electricity networks, in a close collaboration with the Energy Community and the regulatory authorities of the other countries. Based on the abovementioned ERE considers cyber security as a common responsibility with the licensee that operate in power sector for uninterrupted supply.

Article 2

Purpose

The purpose of this document is to define the rules and measures that shall be taken from the operators of critical infrastructures in the power sector for the risk of violating or damaging these critical infrastructures within the framework of the operation through various digital platforms.

Article 3
Object

This regulation defines the obligation of the operators that operate critical infrastructures in power sector to obtain the appropriate measures during the projection, installation and network operation or the equipments used from them, to guarantee the security, integrity and sustainable operation of the power system, as well as to submit at ERE, according to Annex no.2 and Annex no.3, each intervention, violation or incident in the security and integrity of their networks of electronic communication or any intervention, damage that considerably impacts the networks operation and/or their service in the implementation of the cyber security measures to protect the critical and important infrastructures for all the licensee in the electricity production, transmission, distribution activities.

Article 4

The terms used on this Regulation

The terms used in this document shall have the meaning set forth in Law No. 43/2015 "On Power Sector" and Law No. 2/2017 "On Cyber Security".

Article 5

General rules and basic principles

1. The strategy for critical infrastructures in power sector is designed in the form of a guideline in conformity with Article 18 of Law No.43/2015 "On Power Sector", Law No. 2/2017 "On Cyber Security" and Council of Ministers Decision No.222, dated 26.04.2018, "On the approval of the Critical Infrastructure Information List and the List of Important Infrastructures of Information", considering that:

a) The purpose of Power Sector Law is to ensure a sustainable electricity supply through the technical legal framework and in accordance with technological developments, Law No.2/2017 "On Cyber Security" aims to achieve a high level of cyber security and preparedness for cyber attacks by defining security measures, rights, obligations and mutual cooperation between critical infrastructure operators involved in the power sector through which licensed services are provided.

b) The operator of critical infrastructures in the power sector shall take appropriate, proportional, technical and organizational measures to internet security to manage the risks submitted for network and information security on which their principal service is supported and to prevent and minimize the impact of incidents in the principal service through partnership and collaboration between the Operators and ERE.

2. This document supports Critical Infrastructure Operators in conformity with the requirements of Law No.2/2017 "On Cyber Security". For the critical infrastructures and bylaws under its implementation and sets out the processes to assist the Nominated Operator of the Critical Infrastructure to demonstrate that they are managing cyber security risks related to the provided services. These processes mainly include:

a. • Self assessment from the Nominated Operator of Critical Infrastructure ,
b. • Identification and drafting of the action plans
c. • Identification and review of the investments plan

2.a The Nominated Operator of the Critical Infrastructure shall submit its self-assessment at ERE and this self-assessment shall include a detailed information of the complete self-assessment of any significant risks identified and any initial risk treatment proposals including the statement of the outcome achieved by identifying it as “Not achieved” or “Partially achieved” and “Achieved” the Operator is not required to submit any supporting evidence where the results are named "Achieved".

This information shall be submitted using the self-assessment reporting model contained in the Annex. No.1.

With the submission of the information ERE when appropriate, can enter into discussion with the Nominated Operator of the Critical Infrastructure - and request additional information on the reported issues to support its assessments. This may include a request for further clarification on the Self Assessment results that are considered "Not Achieved" or "Partially Achieved".

If the related information is not clear ERE can request clarification from the Nominated Operator of the Critical Infrastructure.

The Nominated Operator of the Critical Infrastructure may at any time request to consult with ERE as soon as possible if it is unsure for the reporting issues. After the self assessment completion, the Nominated Operator of the Critical Infrastructure, it shall consider the areas for improvement.

On the initial self-assessment, the main purpose is that the Nominated Operator of the Critical Infrastructure shall undertake a correct self-assessment and develop an improvement plan, where improvements are required. Any assessment of the respective achieved or not achieved status shall be accompanied with the relevant explanations for each conclusion. These reports may be part of the Nominated Operator of the Critical Infrastructure audits and inspections.

2.b Following the Self-assessment process set out above, the Nominated Operator of the Critical Infrastructure shall develop their own action plans. The Nominated Operator of the Critical Infrastructure may require cooperation with ERE as set out above.

The action plans shall be based on the Nominated Operator of the Critical Infrastructure Self-assessments identifying the risks in accordance with their risk management and risk methodology. The improvement plan shall set out cyber security countermeasures that the Nominated Operator of Critical Infrastructure aims to take where the risk is accessed higher taking into consideration the tolerance levels to the risk. The action plans may amongst others include short-term or long-term strategic measures, for which the budget shall be reaccessed through business planning. ERE, may case-by-case, require review of the actions plan from the Nominated Operator of the Critical Infrastructure in order to assist them in prioritizing and planning cyber risk protection.

2.c The Nominated Operator of the Critical Infrastructure needs to develop a Cyber Security Management System, to manage risks appropriately. This system shall be provided within the term set by ERE according to the analysis and proposal of the Nominated Operator of the Critical Infrastructure and may include, among other things, the recruitment of experts in the information technology area and various training. The timeframes for cyber security initiatives and countermeasures shall be part of the improvement plan. The priority of the security measures in the Internet for high risks should be based on the dependency report, the case by case complexity. This may include:

a) Revision of contractual obligations for third parties
b) Establishment of practices for engineering laptops,
c) Establishment of practices for the usage of removable media,,
d) Managing the change of default user accounts and passwords etc.

3. After presenting the first self-assessment and improvement plan, ERE shall perform on-site audits / monitoring.

Article 6

Obligations of the critical infrastructures operators

1. For this strategy the obligations of the critical infrastructures operators in the power sector include:

a. A Nominated Operator of the Critical Infrastrucutre shall take the technical and organizational measures to manage the risks that may arise and that are connected with the network and information systems security on which it is supported the service licensed by ERE, to ensure the continuity of these services.
b. A Nominated Operator of the Critical Infrastructure shall take the measures to prevent and minimize the impact of incidents affecting network and information systems security used to provide the service for which they are licensed by ERE, to ensure the continuity of these services.
c. A Nominated Operator of the Critical Infrastructure is obliged to inform the incidents at ERE and the Authority designated in conformity with Law No. 2/2017 "On Cyber Security". The notification shall be for each incident which has an important effect on the continuity of service, for the licensed activity.

2. In accordance with the definitions on point 1 of this Article, the Nominated Operator of the Critical Infrastructure , shall periodically report once in 6 months, within the months January and July for the preceding 6 months, according to Anex 1 of this regulation for the issues related to the implementation of letter a, and b point 1 of this article and in any other case shall inform as soon as possible and not later than 72 hours from the day when the Nominated Operator of the Critical Infrastructure () was awared for the occurrence of the incident identified according to letter c point 1 of this article.

3. The main factors for accessing the realization by the Operator of the obligations according to this strategy, shall include an assesment by ERE:
- if are implemented or not the appropriate and proportional measures of the security for the security obligations of the Nominated Operator of the Critical Infrastructure.
- if these incidents are notified to ERE

The frequecy of incident occurrence according to letter c, point 1, article 6 itself shall not indicate a failure by operator to fulfill its security and notification obligations.

4. Within 30 days from the incident of critical infrastructures, the Nominated Operator of the Critical Infrastructure shall submit a general report for ERE. Within 60 days from the infrastructures incident being reported by a Nominated Operator of the Critical Infrastructure, the latter shall submit an investigation report after the incidents. In any case the Nominated Operator of the Critical Infrastructure may request the revision of the dates according to this point.

Article 7

Reporting

Criticalal infrastructures shall report not later than 3 working days from the moment of discovering the security incident for each case that constitutes a breach/interference that has violated the cybersecurity of the criticalal infrastructures that the licensee operates.
The working group held by ERE from the representatives of technical directories, with the submission of the information from the licensee in case of reported incidents, shall discuss the reported case with the licensee to assess:
-If the incident is caused because of the actions or inactions of the operator,
-Regarding the need to review the regulatory acts or the need to be supported from other law enforcement institutions for the proposed actions to avoid or reduce the number of incidents.
In conformity with the information prepared by the working group and its analysis, ERE Board may require additional audits and/or inspections to ensure that these actions are correctly addressed.
ERE may require detailed information to support any assessment regarding the compatibility of the licensee actions with the rules regarding the security of the criticalal infrastructures.

If ERE concludes that the cooperation with Nominated Operator of Critical Infrastructure has not operated or it is clear that there are not taken the necessary measures to avoid the incidents on the criticalal infrastructure, ERE shall inform the operator according to the notification which contains:

- The identified evidences,
- The undertaken steps to correct the failures and the time period on which they shall be realized.

Article 8

Penalties

If the licensee does not act in conformity with the action plan, to him shall be implemented the sanctions in conformity with article 107 of Law 43/2015 “On Power Sector ” as well as the “Regulation on the Procedures of Imposing and Reducing the Fines” approved with ERE Board Decision

Article 9

Final provisions

it is approved by ERE Board with Decision no. 235 on December 20-th 2019.

ANNEX NO.1

Self Assessment Report on Criticalal Infrastructure Protection and Risk Management

The Operator shall report on:

Information Security Policies of the criticalal infrastructures that he operates,

Risk Management,

Security roles and responsibilities which include the ability to discover the Incidents and the Ability to Regulate the Consequences,

Security of other parties assets contracted by the licensee,

Personnel qualifications for identifying and responding to cyber attacks.

The Organizational Measures of the:

a) security of information management,
b) risk management,
c) security policies,
ç) organizational
security,
d) security requirements for third
parties,
dh) asset management,
e) human resources security and access of the persons,
ë) events of security and managing cybersecurity incidents,
f) management of work continuation,
g) control and audit,

Technical measures of the:

a) physical security,
b) integrity protection of the communication grids,
c) verifying the users identity,
ç) management of the access authorization,
d) the activity of the administrators and the users,
dh) disclose cyber security events,
e) means for tracking and accessing cyber security events,
ë) applications security,
f) of the cryptographic devices,
g) security of industrial systems.

ANNEX NO.2

The form of reporting a security incident and/or violation of integrity	
Contact Information	*Name of the Entrepreneur:*
	Name and Surname of the person charged for the elimination of security incidents and/or violating integrity:
	Job position:
	Address:
	Phone numbe, e-mail:
Describing the Security Incident and/or Violating the Integrity	*Type:*
	Defining which networks, systems or services are affected by the security incident:
	Occurrence and duration:
	Information about the initial cause or causes:
	Description of the incident (define the data in a detailed way):
	The approximate number of the users affected by the security incident or violating the integrity or their percentage (%) from the total users of the network and/or service:
	Geographical Area affected by the security incident and /or violation of integrity (km²):
	Affected sources
	Consequences:

Management of the security incident and/or violation of integrity	*The undertaken actions (planned to be undertaken) to eliminate the security incident and to reduce its consequences:*
	The measures after the incident
Other important information	*The lessons learned from them*
Data	
The form is submitted to the Responsible Authority by: *E-mail (scanned version) on: incidente.raportimi@ere.gov.al*	

ANNEX NO.3

Self-assessment report of the Operator on the Security Incident impact		
Duration of the security incident (interruption of the service, interception of the communications, malicious software, modification of the data)	*More than one hour, but less than 2 hours*	*Less than two hours*
Number of the users affected from the incident or their % to the total number of the users		
➢ **5%**	*Average*	*High*
In case of an unknown number of users affected by the security shall be assessed, the geographical area of the security incident extent		
>20 km²		
Final Assessment of the Impact:	**Average**	**High**