ENERGY REGULATOR AUTHORITY

REGULATION ON CYBER SECURITY OF CRITICAL INFRASTRUCTURES IN THE POWER SECTOR

Approved with ERE Board Decision No. 126, of date 30.07.2020

Article 1

Authority

Energy Regulatory Authority above other objectives defined on article 18 of Law No. 43/2015 "On Power Sector", as amended, has the promotion and establishment of an internal competitive market, 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 Energy Community and the regulatory authorities of the other countries. Article 26 of Law no. 43/2015, also defines that the power system shall operate as an integrated system with continuous processes of electricity production, transmission, distribution and electricity consumption. Based on the abovementioned ERE considers cyber security in the power sector as an essential element for the maintenance of security and integrity of the Albanian power system.

Article 2

Purpose

The purpose of this regulation is to define the rules and measures that shall be taken from the entities Licensed by ERE on Power Sector which are responsible to guarantee cybersecurity in critical infrastructures that they own and operate. Guarantee of cyber security in the power system ensures the uninterrupted supply with electricity for the customers in our country.

Article 3

Object

This regulation defines the obligation of the operators that operate critical infrastructures in the power sector to establish appropriate measures during the design, installation and network operation or the equipments used from them, to guarantee the security, availability, integrity and sustainability of the operations of the power system. The operators shall submit at ERE according to Annex no.2 and Annex no.3, the reports on each unplanned intervention, violation or incident in the scope of the security, availability and integrity of their electronic communication networks, as well as any intervention, damage that considerably impacts the networks operation and/or their service status.

Adresa: Blvd "Bajram Curri, Rr. Viktor Eftimiu 1023 Tiranë; Tel: +355 42 69 590; E-mail erealb@ere.gov.al
www.ere.gov.al

Article 4

Definition of the Terms

The terms used on this regulation shall have the meaning as follows any other term used on this regulation shall have the meaning defined on Law No. 43/2015 "On Power Sector" as amended, or Law No. 2/2017 "On Cyber Security".

1. "CSIRT" - means the Computer Security Incident Response Team.

2. "Sectoral CSIRT" - means the team / person responsible for Cyber Security Incidents, in the structure of an operator that manages critical and important information infrastructure.

3. "Cyber Space" – means the digital environment capable of creating, processing and processing exchange information generated by systems, information society services, as well and electronic communication networks.

4. "Cyber security Incident" – means a cyber security event during which there is a violation of the security of services or information systems and networks communication and brings a real negative effect.

5. "Critical Information Infrastructure" - means the entirety of networks and systems information, the violation or destruction of which would have a serious impact on health, security and / or economic well-being of citizens and / or the effective functioning of economy in the Republic of Albania.

6. "Critical Information Infrastructure Operator" - means a legal person, public or private private sector, which administers critical information infrastructure and opetare in the power sector TSO s.a., DSO s.a., and KESH s.a..

7. "Cyber Security Risk" - means a circumstance or event, identifiable in reasonable way, which can cause the security of the service or security information systems and communication networks.

8. "Information Security" - means the provision of confidentiality, integrity and confidentiality availability of information.

9. "Cyber Security" - means all legal, organizational, technical and legal remedies educational, in order to protect the cyber space.

10. "ICS" – Information and Comunication Sistems.

11. "NAECCS" – means the "National Authority for Electronic Certification and Cyber Security"

Article 5

General rules and basic principles

1. The regulation for cyber security in critical infrastructures on the power sector is drafted

Adresa: Blvd "Bajram Curri, Rr. Viktor Eftimiu 1023 Tiranë; Tel: +355 42 69 590; E-mail erealb@ere.gov.al
www.ere.gov.al

in conformity with Article 18 of Law No.43/2015 "On Power Sector" as amended, Law no.2/2017 "On Cyber Security" and Council of Ministers Decision No.553, dated 15.07.2020, "On the approval the Critical Infrastructure Information List and the List of Important Infrastructures of Information", considering that:

a. The purpose of Law no. 43/2015 "On Power Sector" as amended is that through the technical and legal framework to be ensured a safe and sustainable electricity supply of the customers in conformity with the technological developments. Law No.2/2017 "On Cyber Security" aims to achieve a high level of cyber security protection and preparedness for cyber attacks by defining security measures, the rights, obligations and mutual cooperation between Critical Infrastructure Operators involved on power sector through which are provided the licensed services.

b. The operator for critical infrastructures on power sector shall take appropriate, proportional, cost effective, technical and organizational measures to guarantee network security, to properly manage, address, and handle appropriately the risks submitted for the networks and information security that they manage in the scope of their activities and having respect to their roles.

2. Above all this regulation serves as a supporting document for the Operators of Critical Infrastructures in conformity with the requests of Law no. 2/2017 "On Cyber Security". For the critical infrastructures and the by-laws implementing it, as well as to decide the processes to help the Critical Information Infrastructure Operator to demostrate and certity that they manage the risks of cyber security related to the provided services. These processes mainly include:

a. Self assessment from the Critical Information Infrastructure Operator,

The Critical Information Infrastructure Operator shall submit its self-assessment at ERE based on the "Regulation on the content and method of documenting security measures (Approved by Order No. 22, dated 26.04.2018 of the National Authority for elektronic certification and cyber security NAECCS). This self-assessment shall include a detailed and complete information (including the used methodology, to realize the self assessment, the approach how this methodology has applied the self-assessment results which shall include the risk identification and mitigation process) of any significant risks identified and any initial risk treatment proposal including the statement of the outcome achieved by identifying it as "Not achieved" or "Partially achieved" and "Achieved".

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

After the submission of the information ERE, when appropriate, ERE may enter into discussions and request additional information on the reported issues to realize the respective assessments. This may include a request for further clarification on the Self Assessment results that are considered "Not Achieved" or "Partially Achieved". If the information submitted at ERE is not clear this last one may require clarification from

Adresa: Blvd "Bajram Curri, Rr. Viktor Eftimiu 1023 Tiranë; Tel: +355 42 69 590; E-mail erealb@ere.gov.al
www.ere.gov.al

the Critical Information Infrastructure Operator.

The Critical Information Infrastructure Operator may be consulted with ERE as soon as possible if it is not secure for the reporting issues. After completing the self assessment, the Critical Information Infrastructure Operator, shall take into consideration the areas for improvement.

On the initial self-assessment, performed by the Critical Information Infrastructure Operator the main purpose is to perform an objective self assessment and based on these results, the Critical Information Infrastructure Operator shall draft an improvement plan, where they are necessary or according to the priorities defined by ERE. Any assessment according to the achieved or not achieved respective status shall be accompanied with the respective explanations for any conclusion. ERE may require that the self assessment reports prepared by the Critical Information Infrastructure Operator to be audited.

b. Identification and drafting of the action plans taking into consideration of the potential and identified risks

Following the self-assessment process set out above, the Critical Information Infrastructure Operator shall propose their own action plans to the regulatory authorities. The Critical Information Infrastructure Operator may require cooperation with ERE as set out above.

The action plans shall be based on the Critical Information Infrastructure Operator self-assessments identifying the risks in conformity with their risk management process and risk methodology. The improvement plan shall set out cyber security action plan that the Critical Information Infrastructure Operator 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 reassessed through appropriate business planning. ERE, may case-by-case, require review of the actions plan from the Critical Information Infrastructure Operator in order to assist them in prioritizing and planning cyber risk protection.

c. **Identification and review of the investments plan that shall take into due consideration the need to mitigate the risks identified at point (2.b).**

The Critical Information Infrastructure Operator needs to develop a Information Security Management System, to manage cyber risks appropriately at each level of the supply system. This system shall be provided within the term set by ERE according to the analysis and proposal of the Critical Information Infrastructure Operator and may include, among other things, the engagement of the experts in the information technology security area as well as different trainings. The terms for initiatives and countermeasures of cyber security shall be part of the improvement plan. The priority of the security measures in the networks for high risks should be based on the self assessment report, case by case.

Adresa: Blvd “Bajram Curri, Rr. Viktor Eftimiu 1023 Tiranë; Tel: +355 42 69 590; E-mail erealb@ere.gov.al
www.ere.gov.al

3. After submitting the first self-assessment and improvement plan, ERE shall carry out on-site monitorings at the Critical Information Infrastructure Operator and following the monitoring results shall submit the respective recommendations.

Article 6

Obligations of Critical Infrastructures Operators

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

   a. A Critical Information Infrastructure Operator 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, refering to "Regulation on the content and method of documenting security measures (Approved by Order No. 22, dated 26.04.2018 of the National Authority for elektronic certification and cyber security NAECCS).

   b. A Critical Information Infrastructure Operator 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. The categories of the Cyber Incidents are defined according to the "Regulation on the Categories of Cyber Incidents and the format & elements of the report (Approved by Order No.22, dated 10.09.2018 of the NAECCS).

   c. A Critical Information Infrastructure Operator shall be responsible to implement the measures that guarantee cyber security from the third parties providing critical infrastructure services or products. The network operators TSO and DSO companies shall be also responsible for the implementation of the cyber security measures from the respective network Users.

   d. A Critical Information Infrastructure Operator 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 conformity with the provisions of point 1 of this article, the Critical Information Infrastructure Operator shall report periodically once in every six months within January and July for the previous six months, according to Annex 1 of this regulation for the issues related to the implementation of the letter a, b and c of point 1 of this article and in any other case shall notify immediately and not later than 4 hours from the moment of detection of the security incident identified according to letter d of point 1 of this article.

3. The main factors for accessing the realization by the Operator of the obligations according to this regulation shall be monitored by ERE. On each case ERE shall access:

Adresa: Blvd "Bajram Curri, Rr. Viktor Eftimiu 1023 Tiranë; Tel: +355 42 69 590; E-mail erealb@ere.gov.al
www.ere.gov.al

- if are implemented or not the appropriate and proportional measures of cyber security according to the Critical Information Infrastructure Operator duties.
- if these incidents are notified to ERE

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

Within 30 days from the incident on critical infrastructures, the Critical Information Infrastructure Operator shall submit a general report for ERE. Within 90 days from the infrastructures incident the Critical Information Infrastructure Operator, shall submit at ERE a detailed investigation report for the incidents.

Also ERE may require to the Critical Information Infrastructure Operator to submit at ERE the audited report regarding the investigation of cyber security incident.

Article 6/1

Other obligations

Critical Infrastructure Operators in the power sector in addition to the obligations defined on article 6 of this regulation, shall take the measures for the implementation of the definitions provided as follows on this article:

1. Implementation of full organisational and technical cyber security measures in the communication and information systems through:
   a. Protection of information critical infrastructure to guarantee the services;
   b. Management of technology assets of communication and information;
   c. Controlling the continuity of the security measures;
   d. Continuous assessment of the security measures;
   e. Reflecting the security requirements for new projects of communication and information systems;
   f. Implementing the protection technologies;
2. Increase the responsibility of critical infrastructure operators for cyber security through:
   a. Drafting and implementation of accurate rules and procedures for the structures responsible for cyber security in Critical Information Infrastructure Operator;
   b. Drafting and implementing the forms and the reporting approaches of reporting cyber attacks for the responsible structures of cyber security at Critical Information Infrastructure Operator;
   c. Development of the capacities and the dedicated structures for cyber security;
   d. Coordination between the structures for the reaction to security attacks;
   e. Exchange of information for cyber security;

Adresa: Blvd “Bajram Curri, Rr. Viktor Eftimiu 1023 Tiranë; Tel: +355 42 69 590; E-mail erealb@ere.gov.al
www.ere.gov.al

3. Developing the level and capabilities of the cyber security specialists and the users of Communication and Information Systems through:
   a. Recruitment and appointing the specialists for cyber security;
   b. Continuous training of the specialists their promotion and certification;
   c. Concepting the training as a complex field where it is included the reaction to the incidents, penetration tests in the systems, risk management, threat analysis, warning approaches;
   d. Cyber protection training in the programs of training the responsible staff for the critical Infrastructures Operators.
4. Increase the cooperation between the critical infrastructure operators in the field of electricity regarding cyber security through
   a. Cooperation according to the definitions of the Cyber Security Protection Policy in Albania;
   b. The obligations of Law no. 2/2017 “On cyber security”;
   c. Participation in cyber security trainings.
   d. Exchange of mutual information regarding cyber security through Critical Information Infrastructure Operator.

Article 7

Sectorial Computer Security Incidents Responding Team (CSIRT)

"Critical Information Infrastructure Operators” in power sector shall define the responsible persons for the coordination, monitoring and implementing cyber security measures. These representatives shall be part of the Team Responding to Computer Security Incidents (Sectorial CSIRT). Appointing the responsible persons for cyber security shall be within 3 months from the effectiveness of this regulation. Also the Critical Information Infrastructure Operators on power sector shall draft the rules and the operation approach of the sectorial CSIRT refering also to the “Instruction for Methodology for organization and functioning of CSIRTs at national level (Article 7, point 3 of Law no. 2/2017 “On Cyber Security”).

Article 8

Reporting

Critical Information Infrastructure Operator in power sector shall report immediately and not later than 4 hours from the moment of detecting the security incident for each case that constitutes a breach/interference that has violated the cybersecurity of critical infrastructures that the licensee owns or operates as well as for any other service that the operator uses from the third parties.

Adresa: Blvd “Bajram Curri, Rr. Viktor Eftimiu 1023 Tiranë; Tel: +355 42 69 590; E-mail erealb@ere.gov.al
www.ere.gov.al

ERE, with the submission of the information from the licensees in case of the reported incidents, shall review the reported case with the licensee to access:

- 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, prevent or reduce the number of incidents.

ERE may require detailed information from the Critical Information Infrastructure Operator to support any assessment regarding the compatibility of the licensee actions with the rules regarding the security of the critical infrastructures.

If ERE concludes that the cooperation with the Critical Information Infrastructure Operator has not operated or it is clear that there are not taken the necessary measures to avoid the incidents on the critical infrastructure, ERE shall inform the operator for the identified failures. ERE may set deadlines to correct the failures evidenced by the Critical Information Infrastructure Operator.

Article 9

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 10

Certification with ISO 27001 security standard

The Operator of the Critical Infrastructure in power sector shall be equiped with the ISO 27001 security standard certificate within 18 months from the effectiveness of this regulation.

Article 11

Final provisions

This regulation becomes effective after the approval and publication of ERE Board Decision in the official gazette.

Adresa: Blvd "Bajram Curri, Rr. Viktor Eftimiu 1023 Tiranë; Tel: +355 42 69 590; E-mail erealb@ere.gov.al
www.ere.gov.al

ANNEX 1

Self Assessment Report on Critical Infrastructure Protection and Risk Management

The Operator based on "Regulation on the content and method of documenting security measures (Approved by Order No. 22, dated 26.04.2018 of the National Authority for elektronic certification and cyber security NAECCS) shall report on:

The Organizational Measures are:

a) Information Security Management,
b) Risk management,
c) Security policies,
ç) Organizational security,
d) Security requirements for the third parties,
dh) Asset management,
e) Human resources security and access of the persons,
ë) Security events and cybersecurity incidents management,
f) Management of work continuity,
g) Control and audit,

Technical measures are:

a) Physical security,
b) Protecting the integrity of communication networks,
c) Verification of user identity,
ç) Management of the access authorization,
d) The activity of administrators and users,
dh) Detecting cyber security events,
e) Tracking and evaluation tools for cyber security events,
ë) Applications security,
f) Cryptographic equipment,
g) Security of industrial systems.

Adresa: Blvd "Bajram Curri, Rr. Viktor Eftimiu 1023 Tiranë; Tel: +355 42 69 590; E-mail erealb@ere.gov.al
www.ere.gov.al

ANNEX 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 number, 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:

Adresa: Blvd "Bajram Curri, Rr. Viktor Eftimiu 1023 Tiranë; Tel: +355 42 69 590; E-mail erealb@ere.gov.al
www.ere.gov.al

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*	

Adresa: Blvd "Bajram Curri, Rr. Viktor Eftimiu 1023 Tiranë; Tel: +355 42 69 590; E-mail erealb@ere.gov.al
www.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 1 hour but less than 2 hours*	*More than 2 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 incident shall be assessed, the geographical area of the security incident extent		
➢ **20 km²**		
Final Assessment of the Impact:	**Average**	**High**

Adresa: Blvd "Bajram Curri, Rr. Viktor Eftimiu 1023 Tiranë; Tel: +355 42 69 590; E-mail erealb@ere.gov.al
www.ere.gov.al