

**REGULATORY COMMISSION FOR ELECTRICITY  
OF REPUBLIC OF SRPSKA  
TREBINJE**

Pursuant to Article 34 of the Law on electricity ("Official Gazette of Republic of Srpska" number 66/02, 29/03, 86/03 and 111/04), Article 34 paragraph 1 of the Statute of the Regulatory Commission for electricity of Republic of Srpska ("Official Gazette of Republic of Srpska" number 41/04) and Article 37 paragraph 1 point 1 of the Procedural Rules of the Regulatory Commission for electricity of Republic of Srpska ("Official Gazette of Republic of Srpska" number 96/04), Regulatory Commission for electricity of Republic of Srpska, in its first regular session which was held on 30 January 2007 made

**RULE BOOK ON CONFIDENTIAL INFORMATION**

**I GENERAL PROVISIONS**

**Article 1  
(Subject)**

Rule book on confidential information (hereinafter Rule) of the Regulatory Commission for electricity of Republic of Srpska (hereinafter REERS) provides the term and types of confidential information, measures and procedures for the confidential information defining, access to and usage and protection of confidential information.

**Article 2  
(Definitions)**

The terms used in this Rule, including those from the Rule book on public hearings and settlement of disputes and complaints shall have the following meaning:

**"Information"** shall mean any materials in writing or e-mail form used for transmission of facts, opinions, data or any other materials including its copy or part of it.

**"Confidential information"** shall mean the information or datum contained in any materials and which was, by law, Decision or other regulation of REERS or other respective body determined as confidential and which, if disclosed to non-authorized persons, may jeopardize the interest or integrity of REERS or other physical or legal persons.

**"Document"** shall mean the written act printed on a sheet of paper or in e-mail form (records, documents, tables, drawings, graphs, etc) or any other documents which contain confidential information.

**"Subject"** shall mean scale model, model, sample, photos, films and other regulations which were in light, sound, mechanic or some other way recorded at certain base.

**"Measures and procedures"** shall mean all types of orders, instructions, notifications and other actions undertaken by authorized persons for the purposes of protection of confidential information.

**"Protection of confidential information"** shall mean physical and material-technical procedural action, activity or procedure with the aim to prevent destruction, abalienation or misuse of confidential information.

**"Usage of confidential information"** shall mean the procedure of confidential information usage by the authorized person while carrying out the activity, protecting the source and access to confidential information.

**"Access"** shall mean the procedure or a possibility to inform persons about confidential information pursuant to the provisions prescribed by this Rule.

### **Article 3 (Confidentiality protection requirement)**

Each person who has an access to or has been informed about in some other way or has confidential information on disposal, is obliged to comply with measures and procedures of the confidentiality protection, prescribed by this Rule.

## **II CONFIDENTIAL INFORMATION**

### **Article 4 (Types of confidential information)**

- (1) Confidential information in the sense of this Rule is official, operational and professional secret.
- (2) Official secret shall mean data or information which was by law, other regulation, general or individual papers of the responsible body in the prescribed procedure, determined as secret datum or confidential information including but not being limited to the sphere of public security, defense, foreign affairs and interests, intelligence and security interests and similar.
- (3) Operational secret shall mean data and documents proclaimed by law, other regulations or general document of the company, institution or other legal person as operational secret and which disclosure, because of their nature and importance, to non-authorized person, would be against its interests and would cause or might have harmful consequences for that person, including but not being limited to the generation secret, results of research or designing work, trade secret and similar.

- (4) Professional secret shall mean the secret that some person has found out while carrying out its duty or profession and it is related to personal or family data guaranteed by human rights and fundamental freedom respect, including but not being limited to the race, national or ethnic origin, political opinion, health condition and similar.

## **Article 5 (Confidential information of REERS)**

Confidential information of REERS is considered:

- a) Documents and information which REERS proclaims as official, operational or professional secret
- b) Information which were determined as confidential by international document, law or other regulation of the respective body of the authorities or REERS
- c) Information which REERS found as confidential from other legal or physical persons during the proceeding before REERS or during the REERS activities conducted within the scope of its competence and for which it determined to be information which requires protection.
- d) Information which, by its own nature does not have the confidentiality nature, but in combination with other information, it is confidential information which should be protected
- e) Information which contains elements of the bid or application for participation in the procedure of the procurement contract assignment until the results of the procurement contract assignment are published.

## **Article 6 (Confidential information of other structures)**

- (1) Confidential information and documents of other subjects submitted to REERS may be:
- a) information determined by law or other regulations as confidential;
  - b) information which is considered confidential or secret according to the law and in a prescribed procedure by the authorized body
  - c) Information determined as confidential and for which it was submitted application for the confidentiality protection to REERS because of a possibility of harmful consequences for the applicant if published
- (2) It can be asked for treatment of confidentiality with the request referred to in the point c paragraph (1) of this Article only for concrete generation, trade or commercial data from the contract or other document while its applicant is obliged to state the basis for confidentiality, to explain the nature of

confidential information and possible damage that would occur if that information is published, and propose the period for protection of the mentioned information.

**Article 7  
(Deviations)**

Datum or information which secrecy or confidentiality is determined with an intention to hide the committed crime, exceeding or misuse of authority with the aim to hide any illegality or administrative mistake cannot have the nature of secrecy or confidentiality.

**III MEASURES AND PROCEDURES FOR THE CONFIDENTIAL INFORMATION PROTECTION**

**Article 8  
(Designation of the confidential document by the applicant)**

- (1) Information which confidentiality was determined by the authorized person of other body, organization or institution and for which it is requested the confidentiality protection by REERS, is submitted, in a sealed envelope and marked as "CONFIDENTIAL" at a noticeable place.
- (2) Documents, which are in a sealed envelope, should contain a designation on the confidentiality level and type of confidential information.

**Article 9  
(Receipt of the confidential document)**

- 1) The mail marked as "CONFIDENTIAL", received at the protocol office, is opened by the president, members of REERS or Chief of Staff authorized by the president.
- 2) The person that opened the mail provides that the documents contained in the mail referred to in paragraph (1) of this Article are marked with a designation for confidential information of REERS and forwards them for further treatment pursuant to provisions of this Rule.
- 3) Depending on the purpose of the submitted documents which contain confidential information, REERS Chief of Staff forwards them to the Chief of the respective sector or Presiding Officer in order to analyze justification of having information treated as confidential.

**Article 10**

**(Estimate of the application for protection of confidential information)**

- (1) Chief of Sector or Presiding Officer analyzes justification of the application to protect the submitted information as confidential pursuant to the provision of Article 6 of this Rule taking into account the importance of information for the REERS transparency.
- (2) If Chief of Sector or Presiding Officer, in consultation with Chief of Staff estimates that the application for protection of confidential information is not justified, he informs the applicant accordingly i.e. participants to the proceeding and leaves them a deadline of three days for objection which they can submit to REERS, for the purposes of deciding on protection of the confidential information.
- (3) REERS makes decision on the objection referred to in paragraph 2 of this Article at the internal meeting which may be attended by the applicant.
- (4) If the person referred to in paragraph (2) of this Article estimates that the application for protection of confidentiality is justified, he informs participants to the proceeding accordingly, members of REERS and Chief of Staff for the purposes of proper designation, recording and further treatment of confidential information.

**Article 11  
(Confidential document designation in REERS)**

- (1) Confidential document and information printed on paper or recorded on some media in a electronic form, are marked with designation "CONFIDENTIAL" on a noticeable place, registered in a special Book, separately stored and kept in a locked cupboard in an official premise with a limited access.
- (2) Designation, registration, storage and keeping of documents referred to in paragraph (1) of this Article are carried out by Protocol administrator.
- (3) Designation of confidentiality of the document containing confidential information is also put on all its Appendices.
- (4) Electronic data base containing confidential information should be marked with designation of confidentiality and ensured with the key from the unauthorized access.

**Article 12  
(Records on confidential information)**

- (1) Documents designated as confidential are kept in the Book of confidential information which contains basic data on confidential information, its reporting, submission, usage and disclosure.

- (2) The book of confidential information is kept within REERS protocol in a way prescribed by the Rule book on office and archive operation of REERS and it is stored and kept along with the document containing confidential information.

#### **IV PROCEEDING RELATED TO PROTECTION OF CONFIDENTIAL INFORMATION**

##### **Article 13 (Confidential information keeping requirement)**

- (1) Members and all REERS employees, as well as other persons who cooperate in any way with or are engaged by REERS, who have found out, in any way, the content of documents or confidential information, are obliged to keep confidential information.
- (2) Confidential information keeping requirement is valid even after the duty, service or employment of persons in REERS.

##### **Article 14 (Access to confidential information)**

- (1) The following parties have an access to confidential information:
  - a) Members of REERS,
  - b) Chief of Staff of REERS,
  - c) Employees, only for the purposes of carrying out their duties, having received authorization and stated that they understood their obligations and consequences which may occur if confidential information is intentionally or negligently possessed by non-authorized person.
  - d) Third parties who were reported confidential information, pursuant to provisions of this Rule, after they had signed the statement on access to confidential information.

##### **Article 15 (Treatment with confidential information)**

- (1) Employees who, while carrying out their duties, handle confidential documents and information must neither make them available to other persons to see or use them, nor give any kind of statements regarding that document or information.
- (2) The employee dealing with creation, typing and multiplying of confidential document and information is obliged to destroy all their drafts and concepts, i.e. to keep its hard copy in a safe way and save the electronic version on the computer and other material which might disclose the content of that document or information.

- (3) Multiplying, copying and making extracts from the documents which contain confidential information may be done only with previously obtained approval of the REERS president or person he authorizes, whereby each copy is marked with an appropriate ordinal number.
- (4) Original copies of confidential documents, upon completion of the proceeding before REERS, may be returned to the subject that submitted them, at his written request.

**Article 16**  
**(Cessation of confidentiality)**

- (1) Confidentiality of information i.e. documents containing confidential information, may cease:
  - a) on certain date,
  - b) upon completion of certain proceeding,
  - c) upon expiry of certain deadline and
  - d) terminating confidentiality by an authorized person
- (2) If, because of the content nature of the document or confidential information, it is not possible to determine the way of confidentiality cessation, its confidentiality ceases upon expiry of the period determined pursuant to the Law on archive activity.

**Article 17**  
**(Destruction of confidential documents)**

- (1) Destruction of the document which contains confidential information, upon expiry of deadline for keeping, is made by the REERS commission in a way which provides for and protects confidential information from disclosure.
- (2) Commission referred to in paragraph (1) of this Article makes the Minutes on destruction of confidential document or information.

**Article 18**  
**(Disclosure of confidential information or disappearance of the document)**

- (1) In case of disclosure of confidential information or disappearance of the document which contains confidential information, the person who finds it out is obliged to inform the responsible person of REERS, without any delay, who shall immediately undertake necessary measures for the purposes of removal of possible harmful consequences and determine circumstances, under which the confidential information was disclosed, i.e. disappearance of the document which contains confidential information.

- (2) Special records are kept on the confidential information disclosed or the document disappeared which contains confidential information.

### **Article 19**

#### **(Submission of confidential information to competent institutions)**

Submission of confidential information to the National Assembly of Republic of Srpska or other responsible institution, through reports approved by REERS shall not be considered disclosure of confidential information.

### **Article 20**

#### **(Reporting of official, operational or professional secret)**

- (1) Confidential information, which was determined as official, operational or professional secret by provisions of this Rule, cannot be reported, submitted or in other way made available, without authorization, or obtained in order to be submitted to non-invited person.
- (2) Non-authorized disclosure of professional secret, disclosure and non-authorized obtaining of operational secret and disclosure of official secret are considered crimes.

### **Article 21**

#### **(Reporting of confidential information)**

- (1) When it is necessary for the purposes of realization of the REERS activities, it may be reported information, whose confidentiality was confirmed by REERS, to the third party with previously obtained consent of the party that asked for confidentiality treatment.
- (2) The consent referred to in paragraph 1 of this Article necessarily contains:
  - a) name and type of the requested information,
  - b) name of the person the confidential information is reported to,
  - c) name of the person who is authorized for reporting,
  - d) reasons why reporting is necessary,
  - e) way in which the requested confidential information is to be reported, i.e. used
- (3) Access to confidential information which is subject of the discussion may be limited to the parties or participants to the proceeding.
- (4) Exceptionally, if it is necessary for the complete and proper determination of the factual state in the proceeding conducted



by REERS in order to make fair decision, confidential information of one participant to the proceeding may be reported, without his consent, to other participants to the proceeding, pursuant to special REERS decision.

- (5) While reporting confidential information or getting briefed on the document which contains confidential information, the person, who reports, is obliged to emphasize that such information i.e. the document is determined as confidential and warn the persons who they are reported to on obligation to keep their confidentiality and responsibility in case of non-authorized disclosure.
- (6) Information on reporting confidential information to the third person is included in the Book on confidential information with the following details:
  - a) Name and function of the person, i.e. name of the body that confidential information is reported to or respective document submitted which contains confidential information
  - b) Content of confidential document and information which was reported and in which volume and time and purpose of the confidential information reporting.

## **Article 22 (Exclusion of the public)**

During any hearings on confidential information, the public is excluded, while participants to the proceeding who were reported confidential information are obliged to keep it and can neither disclose it to anybody nor can they use that information for any other purposes.

## **IV VIOLATION OF OBLIGATION TO KEEP CONFIDENTIAL INFORMATION, RESPONSIBILITY AND SUPERVISION**

### **Article 23 (Violation of obligation to keep confidential information)**

Violation of obligation to keep confidential information is considered by:

- a) Any dealing with confidential information or document that contains confidential information and which is against this Rule provisions,
- b) Non-authorized reporting, submission or making document and confidential information available in some other way,

- c) Obtaining confidential information or document for the purposes of non-authorized submission;

**Article 24  
(Exceptions)**

- (1) Reporting of information proclaimed confidential is not meant by violation of duty if such reporting is made to physical or legal persons who may or must be reported such information, as follows:
  - a) pursuant to the Law and other regulations,
  - b) pursuant to competence resulting from the duty they deal with, position they hold or job they have, i.e. competences of those legal persons,
- (2) Reporting of confidential information at REERS sessions is not considered violation of duty if such reporting is necessary for realization of duties and carried out pursuant to Article 14 of the Procedural rules of the Regulatory Commission for Electricity of Republic of Srpska;
- (3) Authorized person that at REERS sessions reports confidential information is obliged to warn those present that such information was proclaimed confidential, and those present are obliged to keep as operational, professional or official secret anything they find out on that occasion.
- (4) Reporting of confidential information in order to notify the crime or violation to the respective body or supervision board for the purposes of realization of their rights from the employment shall not be considered violation of the duty.

**Article 25  
(Responsibility for violation of obligation to keep confidential information)**

- (1) Violation of the obligation to keep confidential information or document which contains confidential information is severe violation of the duty - for REERS employees - that is penalized pursuant to the rules and regulations of REERS.
- (2) Violation of the obligation to keep confidential information is unconscientiously and negligibly violation of the assigned duties, as well as violation of the Ethic code provisions for the members and employees in the Regulatory Commission for electricity of Republic of Srpska, for which violation it may be taken disciplinary action against - cessation of the duty.

- (3) Responsibility of the employee that makes severe violation of the duty referred to in paragraph (1) and (2) of this Article is determined pursuant to provisions of the Rule on work, internal organization and systematization of positions of the Regulatory Commission for electricity of Republic of Srpska and may be the basis for cancellation of the Contract on employment.
- (4) If, due to non-authorized reporting of the confidential information, the damage occurs, it may be initiated the proceeding for the damage reimbursement against the responsible person.

**Article 26**  
**(Supervision over the confidential information protection)**

Supervision over the confidential information protection is made by the REERS president or a person authorized by the president.

**V TRANSITIONAL AND FINAL PROVISIONS**

**Article 27**  
**(Getting briefed the staff on provisions of the Rule)**

- (1) All REERS employees who may be in a contact in any way with confidential information or documents which contain confidential information are obliged to get briefed directly on provisions of this Rule and to provide for its appropriate application.
- (2) All REERS employees in case of non-compliance to provisions of this Rule are obliged to undertake appropriate measures immediately.

**Article 28**  
**(Authorization for access to confidential information and statement)**

- (1) REERS president shall, within 8 days from the Effective date of this Rule, prescribe the form and content of the Authorization for access to confidential information and Statement referred to in Article 14 point c) and d) of this Rule.
- (2) Records of the authorizations and statements issued, referred to in paragraph (1) of this Article, are kept by the Protocol Administrator.

**Article 29**  
**(Interpretation of the Rule provisions)**

- (1) In case of discrepancies in application of some provisions of this Rule, the interpretation is to be provided by REERS.

(2) Amendments of this Rule are made, in a way and proceeding determined for its making.

**Article 30**  
**(Effective date and publishing)**

This Rule becomes effective on the eighth day from the day it was published in the "Official Gazette of Republic of Srpska".

REERS president  
Milenko Cokorilo

Number 01- 49-1/07  
30 January 2007  
Trebinje