هيئة تنظيم الاتصالات
Telecommunications Regulatory Authority
Kingdom of Bahrain – مملكة البحرين

PROMULGATING THE NEW REGULATION AND CONDUCTING A PUBLIC CONSULTATION

A public consultation document issued by the Telecommunications Regulatory Authority of the Kingdom of Bahrain on Risk Management of Critical Telecommunications Infrastructure: (the "**Critical Telecommunications Infrastructure Risk Management Regulation**").

21 January 2016

Ref: CSD/0116/006

The address for responses to this document is:

The General Director
Telecommunications Regulatory Authority
PO Box 10353
Manama
Kingdom of Bahrain

Alternatively, e-mail responses may be sent to CSD@tra.org.bh

The deadline for responses is 21 February 2016.

Purpose: to seek stakeholders' views on a proposed new Regulation on Risk Management of Critical Telecommunications Infrastructure: (the "**Critical Telecommunications Infrastructure Risk Management Regulation**").

1 INSTRUCTIONS FOR SUBMITTING A RESPONSE

1.1 The Telecommunications Regulatory Authority (the "**Authority**") invites comments on this consultation document from all interested parties. Comments should be submitted no later than 4pm local time on the 21st of February 2016.

1.2 Responses should be sent to the Authority preferably by email (either Word or PDF format) or by fax or post to the attention of:

The General Director
CSD@tra.org.bh
Telecommunications Regulatory Authority,
P.O. BOX 10353, Manama, Kingdom of Bahrain
Fax: +97317532125

1.3 Responses should include:

- the name of the responding entity;
- the name of the principal contact person;
- full contact details (physical address, telephone number, fax number and email address);
- in the case of responses from individual consumers, name and contact details; and
- a brief statement explaining the interest of the responding entity.

1.4 The Authority seeks comments from stakeholders in the telecommunications industry, the business community and the general public on the proposed new Critical Telecommunications Infrastructure Risk Management Regulation (the "**New Regulation**"), attached at Annex 1. All comments should be supported as much as possible by detailed explanation, including, where relevant, references to the specific provisions of the Telecommunications Law[1] or Licences that the respondent is relying upon.

[1] The Telecommunications Law of the Kingdom of Bahrain, promulgated by Legislative Decree No. 48 of 2002

1.5 Further, the Authority invites respondents to provide comments in response to each of the questions listed for reference at Annex 2.

1.6 In the interests of transparency, the Authority intends to make all submissions received available to the public, subject to the confidentiality of the information received. The Authority will evaluate a request for confidentiality in line with the relevant legal provisions[2] and the Authority's published guidance on the treatment of confidential and non-confidential information[3].

1.7 Respondents are required to mark clearly any information included in their submission that is considered confidential. Where such confidential information is included, respondents are required to provide both a confidential and a non-confidential version of their submission (in soft copies and not scanned copies). If part or all of the submission is marked confidential, reasons should be provided. The Authority may publish or refrain from publishing any document or submission at its sole discretion.

[2] Including Article 23 of the Telecommunications Law

[3] http://www.tra.org.bh/media/document/Confidentiaity_Guidelines_Final.pdf

ANNEX 1:

DRAFT CRITICAL TELECOMMUNICATIONS INFRASTRUCTURE RISK MANAGEMENT REGULATION

Preamble

This Regulation is issued by the Telecommunications Regulatory Authority (the "Authority") of the Kingdom of Bahrain pursuant to the provisions of the Telecommunications Law promulgated by Legislative Decree No. 48 for the year 2002 (the "Telecommunications Law").

Article 3(b) of the Telecommunications Law specifies that the Authority should undertake its duties in relation to Telecommunications services in the manner best calculated to protect the interests of Subscribers and Users in respect of, among other things, the availability and provision of service, the quality of services, and the protection of the personal particulars and privacy of services.

Article 3(e) of the Telecommunications Law states that the Authority shall act in a manner that is consistent with the objectives of the National Plan for Telecommunications; provided that this shall not be construed to derogate from the independence of the Authority in the fulfilment of its duties and the exercise of its powers.

Section 7.7 of the Third National Plan for Telecommunications requires continuous review of the security of critical national infrastructure and the formulation and testing of plans to respond to and recover from disasters for national communications infrastructure.

1 DEFINITIONS

1.1 Any word, phrase or expression used in this Regulation shall, unless it is expressly defined herein, have the same meaning as in the Telecommunications Law of the Kingdom of Bahrain, Legislative Decree No. 48 of 2002.

1.2 References to time are references to time in the Kingdom of Bahrain measured using the 24 hour clock.

1.3 The terms and phrases below shall have the following meaning, unless the context requires otherwise:

Term	**Definition**
Affected Licensee:	Any Licensee that receives a Risk Management Determination.
Assessor:	A natural person or a juristic entity certified ISMS lead auditor based on ISO 27001 standard to assess and audit the Information Security Management Systems.
Asset Inventory:	Register of the Critical Telecommunications Infrastructure's assets that will be subject to the ISO 27001 standard requirements.
Certification Audit:	An audit conducted by an independent Assessor for the Affected Licensee to certify its Critical Telecommunications Infrastructure under ISO 27001 standard requirements. The outcome of this audit is called a "Certification Audit Report".

Critical Telecommunications Infrastructure:	Any telecommunications Infrastructure which is essential in supporting key sectors of the society and economy.
Disaster Recovery Plan:	A documented process or set of procedures to recover the Critical Telecommunications Infrastructure in the event of a disaster. The Disaster Recovery Plan shall include, but not be limited to, a set of procedures to be undertaken by the Affected Licensees to respond, recover and return the Critical Telecommunications Infrastructure to an accepted level of operations following a disaster.
Incident:	An unwanted or unexpected event in which an Infrastructure is significantly damaged or rendered unavailable.
Infrastructure:	The basic physical and organizational systems and facilities (e.g. buildings, network equipment, power supplies, people and processes) needed for the operation of a Public Telecommunications Network.
ISMS:	Information Security Management System as defined in ISO 27001.
ISO:	International Organization for Standardization.
Risk Assessment:	A systematic process of evaluating the potential Risks to the Critical Telecommunications Infrastructure.
Risk Management Determination:	A determination issued by the Authority pursuant to Article 4 of this Regulation.
Risk Management Process:	A coordinated set of activities and methods that are used to direct the Affected Licensee to control the Risks posed on its Critical Telecommunications Infrastructure.
Risk:	Potential threats that could exploit vulnerabilities in a Licensee's Infrastructure, leading to the unavailability of its Infrastructure.
Safeguard:	A measure that provides protection from damage to ensure the security and availability of the Critical Telecommunications Infrastructure. The term "Safeguarded" and "Safeguarding" shall be construed accordingly.
Security Breach:	Any unauthorized access to data, applications, networks and/or facilities that results in a potentially significant impact on the operation of an Infrastructure.

Surveillance Audit:	A periodic audit conducted by an independent Assessor for the Affected Licensee to ensure that its Critical Telecommunications Infrastructure meets the ISO 27001 standard requirements. The outcome of this audit is called a "Surveillance Audit Report".

2 OBJECTIVES

2.1 The objectives of this Regulation are to:

a) establish a Risk Management Process for the identification and designation of Critical Telecommunications Infrastructure;

b) establish a common approach to assess and protect the security and availability of Critical Telecommunications Infrastructure;

c) define the responsibilities and obligations of Licensees in relation to the management of Risks; and

d) define the responsibilities and obligations of Affected Licensees in relation to the Risk Management Process of their Critical Telecommunications Infrastructure.

3 OBLIGATIONS ON ALL LICENSEES

3.1 All Licensees shall take all appropriate:

a) measures to manage Risks to the security and availability of its Infrastructure; and

b) steps to protect, so far as possible, the security and availability of its Infrastructure.

3.2 A Licensee shall notify the Authority within twenty four (24) hours after becoming aware of any Security Breach or Incident.

3.3 A Licensee shall submit a detailed report to the Authority within five (5) working days after becoming aware of any Security Breach or Incident.

3.4 The notification and detailed report referred to in the preceding Articles 3.2 and 3.3 shall be submitted to the Authority as may be prescribed by the Authority from time to time.

3.5 The detailed report submitted pursuant to Article 3.3 shall include the following information:

a) the date and time that the Security Breach or Incident commenced;

b) the date and time that the Security Breach or Incident was resolved completely. Where the incident is ongoing at the time of reporting, the resolution time shall be provided when it is available;

c) location information, which, as a minimum, shall contain the address; and

d) a brief description of the Security Breach or Incident, including the cause, resultant damage, the estimated financial loss and mitigation action taken so far by the Licensee.

3.6 Where the Authority receives a report under this Article, the Authority may, where it thinks it appropriate, inform:

a) the public of the occurrence of the Security Breach or Incident, or require the Licensee to inform the public; and/or

b) security organs or concerned government entities of such report.

4 RISK MANAGEMENT DETERMINATION

4.1 The Authority shall issue a Risk Management Determination to Licensees that:

a) hold an Individual Mobile Telecommunications Licence (IMTL);

b) hold an International Telecommunications Facilities Licence (IFL); or

c) install, operate and/ or manage a Critical Telecommunications Infrastructure as may be designated.

4.2 The Authority will, in designating Affected Licensee under Article 4.1(c), take into account the following criteria:

a) the criticality of the Affected Licensee's Infrastructure in supporting key sectors of the society and economy;

b) the impact of unavailability of the Affected Licensee's Infrastructure on key sectors of the society and economy; and

c) the financial losses on key sectors of the society and economy resulted in the disruption of the Affected Licensee's Infrastructure.

4.3 The Risk Management Determination shall, at a minimum, include:

a) the justification of designating a Licensee as an Affected Licensee;

b) the documents to be submitted by the Affected Licensee pursuant to Article 5 of this Regulation;

c) general specifications of the Infrastructure elements; and

d) an initial list of types of threat.

5 OBLIGATIONS ON AFFECTED LICENSEES

5.1 Upon receipt of the Risk Management Determination**,** Affected Licensees shall undertake a Risk Management Process in accordance with the Risk Management Determination and in accordance with Articles 5.1.1, 5.1.2, 5.1.3 and 5.1.4 of this Regulation.

5.1.1 Within three (3) calendar months from the receipt of the Risk Management Determination, the Affected Licensee shall:

a) identify its Critical Telecommunications Infrastructure in the Asset Inventory document; and

b) provide the Authority with its Asset Inventory document in accordance with the Risk Management Determination.

5.1.2 Within eighteen (18) calendar months from the receipt of the Risk Management Determination from the Authority, the Affected Licensee shall develop, implement, obtain, maintain and provide the Authority with the following:

a) Disaster Recovery Plan;

b) ISO 27001 certification;

c) Certification Audit Report for the ISO 27001; and

d) Risk Assessment report carried out for the Certification Audit.

5.1.3 The Affected Licensee shall, on an annual basis after obtaining ISO 27001 certification, provide the Authority with the following documents:

a) the Surveillance Audit Report for the ISO 27001;

b) the report of the Risk Assessment carried out for the Surveillance Audit; and

c) the updated Disaster Recovery Plan, if any.

5.1.4 The Affected Licensee is required to attain ISO 27001 re-certification every three (3) years from the date of obtaining ISO 27001 certification and to inform the Authority of such re-certification.

6 ADDITIONAL RISK ASSESSMENTS

6.1 The Authority may request the Affected Licensee to carry out an additional Risk Assessment in the event that the Authority considers that its Critical Telecommunications Infrastructure is not sufficiently Safeguarded.

6.2 Where the Authority request an additional Risk Assessment under Article 6.1, the Affected Licensee shall complete and provide the Authority with its additional Risk Assessment report within three (3) calendar months from the Authority's request, unless otherwise directed by the Authority in writing.

7 ADDITIONAL SAFEGUARDS

7.1 The Authority may, after reviewing the documents provided by the Affected Licensee under Articles 5, 6 and 8 of this Regulation, require the Affected Licensee to implement within three (3) calendar months additional Safeguards intended to further mitigate Risks to the Critical Telecommunications Infrastructure.

7.2 The Affected Licensee shall promptly confirm in writing to the Authority upon completing the implementation of those Safeguards identified under Article 7.1.

8 INADEQUATE RISK MANAGEMENT PROCESS

8.1 In the event that the Authority considers any of the documents submitted under Articles 5, 6 and 7 by the Affected Licensee to be inadequate, the Authority has the right to appoint an independent Assessor to identify any deficiencies. The Affected Licensee shall bear the cost of the independent Assessor.

9 ENFORCEMENT

9.1 Without prejudice to the Authority's power under Article 8, Licensees that fail to comply with the provisions of this Regulation shall be deemed in material breach of the Telecommunications Law.

10 COST

10.1 Each Affected Licensee shall be responsible for the costs of undertaking its obligations under this Regulation including the costs of undertaking an additional Risk Assessment under Article 6 and implementing additional Safeguards under Article 7.

11 CONFIDENTIALITY

11.1 The Authority shall treat all information submitted to it pursuant to this Regulation in accordance with the relevant provisions of the Telecommunications Law and any Guidelines issued by the Authority.

11.2 Licensees shall take all necessary actions to ensure the privacy and confidentiality of the Information obtained in the process of implementing this Regulation. Disclosure of this Information shall only be permitted in accordance with the Laws of the Kingdom of Bahrain.

ANNEX 2: CONSULTATION QUESTIONS

1 ARTICLE 1: DEFINITIONS

1.1 Do you consider the definitions of Article 1 of the Regulation sufficient? If not, please give reasons and state which terms you think should be added or omitted.

2 ARTICLE 2: OBJECTIVES

2.1 Do you agree with the provisions of Article 2 of the Regulation? If not, please give reasons why.

3 ARTICLE 3: OBLIGATIONS ON ALL LICENSEES

3.1 Do you agree with the provisions of Article 3? If not, please give reasons why. In particular:

3.1.1 Do you agree that all Licensees should take all appropriate:

(a) measures to manage Risks to the security and availability of its Infrastructure; and

(b) steps to protect, so far as possible, the security and availability of its Infrastructure? If not, please give reasons why.

3.1.2 Do you agree that all Licensees should be obliged to notify and report to the Authority about Security Breaches and Incidents? If not, please give reasons why.

3.1.3 Do you agree with the information to be reported? If not, please give reasons why.

3.1.4 Do you agree with the timescales for notification and reporting? If not, please give reasons why.

3.1.5 Do you agree that the Authority may, where it thinks it appropriate, inform:

(a) the public of the occurrence of the Security Breach or Incident, or require the Licensee to inform the public; and/or

(b) security organs or concerned government entities of such report? If not, please give reasons why.

4 ARTICLE 4: RISK MANAGEMENT DETERMINATION

4.1 Do you agree with the provisions of Article 4 of the Regulation? If not, please give reasons why.

5 ARTICLE 5: OBLIGATIONS ON AFFECTED LICENSEES

5.1 Do you agree with the provisions of Article 5? If not, please give reasons why. In particular do you agree with the obligations on Affected Licensees associated with:

5.1.1 Identifying its Critical Telecommunications Infrastructure and providing an Asset Inventory document within 3 months from receiving the Risk Management Determination from the Authority?

5.1.2 Developing, implementing, obtaining, maintaining and provide the Authority with the following documents within 18 months from receiving the Risk Management Determination:

(a) Disaster Recovery Plan;

(b) ISO 27001 certification;;

(c) Certification Audit Report for the ISO 27001; and

(d) Risk Assessment report carried out for the Certification Audit?

5.1.3 Providing the following documents on annual basis after obtaining ISO 27001 certification to the Authority:

(a) the Surveillance Audit Report for the ISMS;

(b) the report of the Risk Assessment carried out for the Surveillance Audit; and

(c) the updated Disaster Recovery Plan, if any?

5.1.4 Recertifying and attaining ISO 27001 every three years?

6 ARTICLE 6: ADDITIONAL RISK ASSESSMENTS

6.1 Do you agree with the provisions of Article 6? If not, please give reasons why. In particular:

6.1.1 Do you agree that the Authority should be able to request for additional Risk Assessments to be carried out if it reasonably believes that a particular Affected Licensee's Critical Telecommunications Infrastructure has not been sufficiently safeguarded?

6.1.2 Do you agree with the timescales for initiating a Risk Assessment?

6.1.3 Do you agree with the timescales for completing a Risk Assessment?

7 ARTICLE 7: ADDITIONAL SAFEGUARDS

7.1 Do you agree with the provisions of Article 7? If not, please give reasons why. In particular:

7.1.1 Do you agree that the Authority may, after reviewing the reports provided by the Affected Licensee pursuant to Articles 5, 6 and 8 of this Regulation, require the Affected Licensee to implement additional Safeguards to mitigate Risks to its Critical Telecommunications Infrastructure?

7.1.2 Do you agree that the Safeguards implemented in this case should be subject to agreement with the Authority?

7.1.3 Do you agree with the timescales for implementing Safeguards?

7.1.4 Do you agree with the reporting requirements associated with additional Safeguards?

8 ARTICLE 8: INADEQUATE RISK MANAGEMENT PROCESS

8.1 Do you agree with the provisions of Article 8? If not, please give reasons why. In particular, do you agree that in the event that the Authority considers any of the Affected Licensee's Risk Management Process to be inadequate in relation to this Regulation, the Authority should be able to appoint an independent Assessor to identify inadequate Risk Management Process?

9 ARTICLE 9: ENFORCEMENT

9.1 Do you agree with the provisions of Article 9? If not, please give reasons why.

10 ARTICLE 10: COST

10.1 Do you agree with the provisions of Article 10? If not, please give reasons why.

11 ARTICLE 11: CONFIDENTIALITY

11.1 Do you agree with the provisions of Article 11? If not, please give reasons why.

12 GENERAL OBSERVATIONS

12.1 What other issues do you think should be included in, or excluded from the Regulation? Please support your comments with detailed reasoning.