هيئة تنظيم الاتصالات
Telecommunications Regulatory Authority

Resolution No (5) of 2017

Promulgating the Regulation on Critical Telecommunications Infrastructure Risk Management

The Telecommunications Regulatory Authority's Board of Directors:

After perusal of:

The Telecommunications Law as promulgated by Legislative Decree No. 48 of 2002، and in particular Articles 3(b) and 3(e) thereof,

Decree No. 47 of 2008 and its amendments with respect to the re-formation of the Telecommunications Regulatory Authority's Board of Directors,

Decision No. 29 of 2016 Promulgating the Fourth National Telecommunications Plan,

And on the basis of the proposal submitted by the General Director of the Telecommunications Regulatory Authority,

And after the approval of the Telecommunications Regulatory Authority's Board of Directors,

The following is decided:

The First Article

The Critical Telecommunications Infrastructure Risk Management Regulation attached herewith is hereby being approved and adopted.

The Second Article

The official Arabic version of the Resolution and Regulation attached hereto shall be published in the Official Gazette and shall come into force on the day following the date of publication.

Chairman of the Authority's Board of Directors
Dr. Mohammed Ahmed Al Amer

Issued on 4 Ramadan 1438
Corresponding to 30 May 2017

Critical Telecommunications Infrastructure Risk Management Regulation

Article (1)

Definitions

A. Unless the context otherwise requires, any word, phrase or expression used in this Regulation shall have the meaning given to it in Article (1) of the Legislative Decree No. 48 for the year 2002 promulgating the Telecommunications Law and the following terms and expressions shall have the following meanings:

Term	**Definition**
Affected Licensee:	Any Licensee to which a Risk Management Determination is issued as per Article (4) of the Regulation.
Assessor:	Every natural person or a juristic entity certified Information Security Management Systems lead auditor based on ISO 27001 standard to assess and audit the Information Security Management Systems.
Asset Inventory:	A documented list of all assets that are identified under the "Critical Telecommunication Infrastructure.
Business Continuity Plan:	A best practice framework to minimize disruption during unexpected events that could bring business to a standstill. The objective of this exercise is improve business resiliency
Certification Audit:	An audit conducted by an independent qualified Assessor for the Affected Licensee to certify its Critical Telecommunications Infrastructure. The outcome of this audit is called a "Certification Audit Report".
Critical Telecommunications Infrastructure:	Includes: a) Any telecommunications Infrastructure which is essential for the maintenance of vital societal functions related to health, safety, national security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact; and b) Any centralised system that stores and process Personal Data.
Indicator of compromise:	Digital artefacts or forensic data that indicate a possible Security Breach. This includes "IP address" of the source of Security Breach and other techniques used by the source to carry out the Security Breach.
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.

ISO:	International Organization for Standardization.
Penetration Testing Exercise	A methodical process that is used to verify the protection controls of an Affected Licensee in order to identify any vulnerabilities that can be exploited by attackers over the cyber space.
Personal Data	Any information relating to identified or identifiable natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by Licensee, in particular by reference to user or subscriber information, identification number, Location Data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity if that person
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 minimize the Risks, which poses threats to the Critical Telecommunications Infrastructure.
Risk:	A probability or threat of damage, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action.
Safeguard:	A measure or control that provides protection from damage to ensure the security and availability of the Critical Telecommunications Infrastructure.
Security Breach:	Any unauthorized access to data, applications, networks and/or facilities that results in disclosure of sensitive information and/or potentially significant impact on the operation of an Infrastructure.
Security Incident:	An unwanted or unexpected event that results in loss of service or unauthorized access due to intentional or malicious activity.
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”.

Telecommunications Law:	The "Telecommunications Law" Promulgating the Legislative Decree No. 48 for the year 2002.

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

Article (2)

Objectives

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 uniform and coordinated approach to assess and protect the security and availability of Critical Telecommunications Infrastructure;

C. define the responsibilities and obligations of Licensees in relation to timely detection of and timely response to Security Incidents and Security Breaches;

D. define the responsibilities and obligations of Licensees in relation to the management of Risks; and

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

Article (3)

OBLIGATIONS ON ALL LICENSEES

A. All Licensees shall:

1. take all appropriate measures to manage Risks to the security and availability of its Infrastructure and take all appropriate steps to protect, so far as possible, the security and availability of its Infrastructure;

2. notify the Authority within twenty four (24) hours after becoming aware of any Security Breach or Security Incident;

3. submit a detailed report to the Authority within five (5) working days after becoming aware of any Security Breach or Security Incident. The detailed report shall include the following information:

a. the date and time that the Security Breach or Security Incident commenced;
b. the date and time that the Security Breach or Security 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, at a minimum, shall contain the address;
d. a brief description of the Security Breach or Security Incident, including the cause, resultant damage, the estimated financial loss and mitigation action taken so far by the Licensee; and
e. any Indicators of Compromise identified during the investigation.

B. 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 Security Incident, or require the Licensee to inform the public; and/or

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

Article (4)

RISK MANAGEMENT DETERMINATION

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

1. hold an Individual Mobile Telecommunications Licence (IMTL);

2. hold an International Telecommunications Facilities Licence (IFL); or

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

B. The Authority will, in designating Affected Licensee under Article 4 (A)(3), take into account the following criteria:

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

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

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

C. The Risk Management Determination shall, at a minimum, include:

1. the justification of designating a Licensee as an Affected Licensee;

2. the required documents from the Affected Licensee pursuant to Article 5 of this Regulation;

3. general specifications of the Infrastructure elements; and

4. an initial list of types of threat.

Article (5)OBLIGATIONS ON AFFECTED LICENSEES

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 the following Articles:

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

1. identify its Critical Telecommunications Infrastructure in the Asset Inventory document; and

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

B. 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:

1. Business Continuity Plan

2. ISO 27001 certification;

3. Certification Audit Report for the ISO 27001; and

4. Risk Assessment report carried out for the Certification Audit.

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

1. the Surveillance Audit Report for the ISO 27001;

2. the report of the Risk Assessment carried out for the Surveillance Audit; and

3. the updated Business Continuity Plan, if any.

4. a copy of incident response plan in line with the requirements of ISO 27001.

D. 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.

Article (6)**ADDITIONAL RISK ASSESSMENTS**

A. 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. This may include a Penetration Testing Exercise carried out by a suitably qualified independent assessor. The Affected Licensee shall bear the cost of the independent assessor.

B. Where the Authority request an additional Risk Assessment under Article 6(A), 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.

Article (7)

ADDITIONAL SAFEGUARDS

A. 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.

B. The Affected Licensee shall promptly confirm in writing to the Authority upon completing the implementation of those Safeguards identified under Article 7(A).

Article (8)

INADEQUATE RISK MANAGEMENT PROCESS

In the event that the Authority considers any of the documents submitted under Articles 5, 6 and 7 of this Regulation 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.

Article (9)

ENFORCEMENT

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. The Authority shall take the measures and sanctions stated in the Telecommunications Law on Licensee violating the provisions of this Regulation.

Article (10)

COST

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 of this Regulation and implementing additional Safeguards under Article 7 of this Regulation.

Article (11)

CONFIDENTIALITY

A. 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.

B. 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.