Telecommunications Regulatory Authority

Decision No. 93/2018.

Promulgating Telecommunications Network Security Regulation

Pursuant to the Telecommunications Regulatory Act issued by the Royal Decree No. 30/2002;

The Executive Regulation issued by Resolution No. 144/2008 ;

The approval of TRA Board of Directors ; and
Based on the exigencies of the public interest;

It is decided:

Article (1)
The provisions of the annexed Regulation shall be enforced with regard to the the telecommunications network security.

Article (2)
This Decision shall be published in the Gazette and shall come into force from the date following its publication.

Issued on: 3rd Rabi ʾal-Thani 1440 H
corresponding to : 11 December 2018

Mohammed Bin Hamad Al-Rumhi
Chairman of TRA Board

Telecommunications Network Security Regulation

Article (1)

In the application of the provisions of this Regulation, the terms and expressions used herein shall express the exact meaning exhibited in both the Telecommunications Regulatory Act and its Executive Regulation, whereas the following terms and expressions shall have the meanings shown against each, unless the text otherwise requires:

1- **Network**: the licensee's telecommunications network.
2- **Security incident**: any security breach or loss of integrity or security of the Network.
3- **Network intrusion**: unauthorized access to sensitive data by way of circumventing security systems.
4- **Managed Services Agreement**: a contract with a third party to operate, maintain or manage the Network.
5- **Managed Services Provider**: a contractor appointed to operate, maintain or manage the Network.
6- **Tier 3 Technical Support**: a level of support that requires equipment and systems supplier specialists' intervention.

Article (2)

The provisions of this Regulation is applicable to all Network components; including the Backbone Network, the Access Network, passwords management policy, switches, upgrades, Domain Name System (DNS) and buildings. The Regulation is also applicable to all Network attached equipment and facilities, Including Content Development Networks (CDN), caching systems (permanent and temporary), and content distribution systems.

Article (3)

The licensee must comply with the following:

1- Implement the necessary technical and administrative measures to manage security risks of telecommunications networks and services contained in the ISO 22301 standard for business continuity and the ITU standards set by the ITU-T X-Series Standards.

2- Conduct regular training for employees engaged in the Network security management and conduct general awareness sessions for other employees, at least once a year.

3- Implement the technical measures required to protect the Network from any potential risks through the internal networks of subscribers.

4- Implement the technical measures required to prevent attempts to scan the Network vulnerabilities.

5- Conduct periodic internal security audits to identify threats and vulnerabilities at the Network and operating system layer, the applications layer and the Licensees 'operations and procedures. This is to ascertain the level of the Network security and to ensure that the network is not breached or accessed by unauthorized person. The Licensee shall conduct an external security audit through the involvement of an independent and experienced third party, at least once a year, after obtaining the approval of the Authority. The licensee shall provide the Authority with the dates of these audits and their results within the period determined by the Authority.

6- Conduct periodic security assessments of buildings, external Network elements, stations and towers, as well as the application layer, servers and systems software in order to identify the probable threats and vulnerabilities. Action must be taken if there is any defect or potential threat at the security of the mentioned elements.

7- Ensure that repairs relating to the security and integrity of the Network are carried out and installed in a timely and effective manner by equipment or systems suppliers

8- Maintain a register of the risks to which the Network and the provided services are exposed to and the incidents occurring within the premises and locations of the Licensee. The Authority shall be provided with a detailed report of the content of this register at least once a year or upon request.

9- Maintain CCTV recordings, building entry/exit records and Intrusion Detection System (IDS) record, and the Licensee shall safely and appropriately keep such recordings and records for at least one year.

10- Notify the Authority of any security incident affecting the integrity of the Network within (24) twenty-four hours of becoming aware of the occurrence of the incident, prepare and submit to the Authority a detailed report of the incident within the (15) fifteen-day period following the date of becoming aware of the occurrence of the incident. This report shall include the procedures followed and the corrective and preventive measures taken in respect thereof. The Authority may, if it deems necessary, inform the public about the security incident that occurred.

11- Notify the Authority immediately, upon occurrence, of any security breach that has a significant impact on the operation of the Licensee's Network and services or attempted security breach capable of having the same impact if it succeeded. In such case, the Authority shall have the right to inform the public of the breach or to request the Licensee to do so in the public interest. In all cases, the Licensee shall notify the Authority of any incidents that may result in disruption or interruption of services.

12- Keep all systems used in the operation and management of the Network (e.g. OSS, NMS, etc.) within the Sultanate.

13- Remote access to the Network is restricted to only Tier 3 Technical Support staff when necessary, for a limited period and after obtaining the approval of the Licensee.

14- Ensure that the Managed Service Provider and its sub-contractors would not operate, manage, maintain or have access to systems or equipment used for the realization of national security requirements or undertake any activities through them.

15- Implement technical measures required to protect telecom networks and services against security incidents.

16- Implement technical measures required to protect the Network equipment and servers.

17- Implement technical measures required to protect its premises and buildings, and restriction of access to the authorized persons.

18- Implement technical measures required to protect beneficiary's data against theft or loss.

19- Implement technical measures required to protect outdoor cable cabinets, fiber distribution hubs (FDH) cabinets and distribution points (DP).

20- Implement technical measures required to protect tower locations and stations (e.g. mobile BTS, submarine landing stations, etc.).

21- Furnish the Authority with data and information whenever required.

Article (4)

The Licensee shall observe the following when entering into a Managed Services Agreement:

1- Ensure that the Licensee remains solely responsible for the Network security, services and buildings.

2- Carry out risk assessments and comply with risk mitigation measures explicitly.

3- Assessment by the Licensee of the Managed Service Provider's ability through a structured process and methodology.

4- Manage the requirements of the Network security, services and buildings continuously. The Licensee shall obtain assurances from the Managed Service Provider that such requirements are met.

5- Carefully manage the Network security, services and buildings during a period in which the Managed Service Provider is changed or its contract is terminated.

6- The Managed Services Agreement shall include the following :

A. Security requirements of the Network, the services and the buildings.

B. Security requirements related to the Managed Service Provider's employees.

C. Requirements for managing access to ICT systems and the permissions granted to users of such systems.

D. Security requirements related to services, beneficiaries, data and systems.

Article (5)

Any reports, data and information provided by the Licensee, in application of the provisions of this Regulation, will be strictly confidential and shall not be accessible to third parties unless the Authority decides to make them available to a third party in order to serve the public interest.

Article (6)

The Authority may, at any time, either by itself or acting through specialised companies in this respect, conduct periodic security audits, in addition to security audits conducted in the event of any security incident at the expense of the Licensee. In all cases, the Licensee shall comply with the directives issued by the Authority in this regard.

Article (7)

Without prejudice to any penalty prescribed by law, the following administrative fines will be imposed on whoever violates the provisions of this Regulation. The fine shall be doubled in case of repetition:

No.	Violation	Fine (Omani Rial)
1	Violation of items (1 or 15) of Article (3)	OMR 200,000 (Omani Rials two hundred thousand)
2	Violation of items (3, 4, 5, 6, 7, 8, 9, 11 or 14) of Article (3)	OMR 30,000 (Omani Rials thirty thousand)

3	Violation of items (2, 10, 12 or 19) of Article (3), or violation of Article (4) or Article (5)	OMR 10,000 (Omani Rials ten thousand)
4	Violation of items (16 or 20) of Article (3)	OMR 20,000 (Omani Rials twenty thousand)
5	Violation of item (17) of Article (3)	OMR 10,000 (Omani Rials ten thousand) + Double the cost of repairing the damage
6	Violation of items (18, 13 or 21) of Article (3)	OMR 100,000 (Omani Rials one hundred thousand)
7	Violation of Article (6)	OMR 150,000 (Omani Rials one hundred fifty thousand)