هيئة تنظيم الخدمات العامة
Authority for Public Services Regulation

DRAFT:

ELECTRICITY METERING SYSTEM CYBER SECURITY REGULATION

13 JULY 2021

Executive Summary

In this document we present a draft cyber security regulation for the Electricity Metering System for Oman. This regulation sets out:

- the objective of the Regulation and associated security standard (the Standard)
- the scope and applicability of the Regulation and standard
- the date from which it will be effective
- definition of terms
- the licensees' obligations
- requirements to comply with the Regulation
- governance.

Full compliance with the Regulation and the Standard will take some time to achieve, but the two documents will set the direction for ensuring that Oman's Electricity Metering System is cyber-secure from end to end.

The proposed draft regulation is presented in the body of this report.

Contents

Executive Summary 2

1 Introduction 4

1.1 Objective 4

1.2 Scope 4

1.3 Applicability 4

1.4 Owner 4

1.5 Effective date 4

1.6 Definitions 4

2 Licensee obligations 5

2.1 General obligations 5

2.2 Compliance and assurance 5

2.3 Governance 6

1 Introduction

1.1 Objective

1.1.1 The objective of this Regulation and the Electricity Metering System Cyber Security Standard (the Standard) is to ensure that the End-to-End Electricity Metering System (the System) is secure from reasonably foreseeable cyber attacks, throughout its lifecycle (design, implementation, testing, operation, decommissioning and disposal) in order to:

(a) Protect the supply of electricity to consumers;

(b) Prevent financial fraud;

(c) Provide accurate consumption data to enable accurate and timely billing;

(d) Protect consumer data;

(e) Protect the integrity, function and trust in the supply system and market; and

(f) Support future changes in the electricity supply system and market.

1.2 Scope

1.2.1 The System is comprised of multiple elements including, but not limited to:

(a) Consumer premises;

(i) Electricity meter;
(ii) Communications hub; and
(iii) In-home display unit;

(b) Telecommunications;

(i) All telecommunications used within the System;

(c) Licensee and central services;

(i) Head End System(s);
(ii) Hardware Security Module(s);
(iii) Unique Transaction Reference Number generator(s); and
(iv) Meter Data Management System(s).

1.2.1 Associated systems for customer relationship management, billing, scheduling, payment, etc. are not included in the scope of this regulation and the Standard.

1.3 Applicability

1.3.1 The Regulation and Standard are applicable to entities providing and supporting any element of the System. (Licensee).

1.4 Owner

1.4.1 The owner of this regulation is the Regulatory Authority.

1.5 Effective date

1.5.1 The Specified Date at which this regulation will come into effect determined by the Regulatory Authority directives.

1.6 Definitions

1.6.1 The following definitions are used in this regulation and the Standard:

(a) **Applicable Standard** is the Electricity Metering System Cyber Security Standard, Oman.

(b) **Authority** is the Regulatory Authority established as per the Laws and Regulations of the Sultanate of Oman, which is the Authority for Public Services Regulation.

(c) **Compromise** means an adverse impact on the confidentiality, integrity or availability of any element of the System or data within the System.

DRAFT

(d) **End-to-End System** (the System) is comprised of the hardware, software, telecommunications, processes and procedures comprising the elements defined in 1.2.1 above.

(e) **Information Security Management System (ISMS)** is the collection of policies, procedures, standards and guidelines which define how risk are understood, the System is protected and monitored, how to respond to and recover if the System is compromised.

(f) **Licence** is an authorisation issued by the Regulatory Authority pursuant to the Sector Law entitling the Licensee to undertake a set of regulated activities.

(g) **Licensee** is a Licensed Distribution System Operator (Licensee) which is the holder of a Distribution Licence in Oman.

(h) **Secure** means that the System as a whole and each element of the System is designed, implemented, operated, monitored and maintained to comply with the Standard, and is resistant and resilient to security incidents.

(i) **Security Auditor** means a body which is independent of the System operator, is suitably qualified and experienced to conduct security audits against the applicable standard and any other relevant standards referenced by the Standard.

(j) **Security Incident** is any accidental or deliberate attempt, whether successful or not, to gain unauthorised access, change the System or data, or bypass security controls of any element in order to compromise the System.

(k) **Specified Date** is any date determined by the Authority. This may be expressed as an absolute date (e.g. 1 September 2021) or a date relative to the Effective Date or another Specified Date (e.g. 12 months from the Effective Date).

(l) **Standard** is the Electricity Metering Cyber Security Standard.

(m) **System** is as defined in paragraph 1.2 above.

2 Licensee obligations

2.1 General obligations

2.1.1 Licensees are required to comply with this regulation and the Electricity Metering Cyber Security Standard (the Standard) within 12 months from the Effective Date.

2.1.2 Licensees are required to:

(a) maintain the security of elements of the System provided by the Licensee in accordance with the Standard; and

(b) assure itself that the security of elements of the System supplied by third parties is in accordance with the Standard.

2.1.3 Licensees must take reasonable steps to ensure that the System is designed, developed, configured, tested, operated, maintained, decommissioned and disposed of in order to ensure it is secure at all times.

2.2 Compliance and assurance

2.2.1 Licensees shall establish an Information Security Management System (ISMS) for the System scope as defined in paragraph (1.6.1e) above.

2.2.2 The Licensees' ISMS is required to be certified by a Security Auditor to International Organization for Standards ISO 27001:2013 (entitled Information Technology – Security Techniques – Information Security Management Systems), and as amended from time-to-time.

2.2.3 Certification is to be obtained within 12 months of the Effective Date or a Specified Date determined by the Authority.

2.2.4 Licensees are required to be audited by a Security Auditor at least annually to ensure continuing compliance and certification.

DRAFT

2.2.5 A copy of each audit report and certificate is to be sent to the Authority within 30 days of issue by the Security Auditor.

2.2.6 The Authority can conduct audits at any time. The Authority can appoint a Security Auditor to conduct the audit on its behalf.

2.2.7 Licensees are required to conduct assurance that the security of services and products from third party suppliers meets the requirements of the Standard within 12 months of the Effective Date or as determined by the Authority, and at least annually thereafter.

2.2.8 The Authority may from time to time issue a direction which requires the Licensee to take action or cease certain activities in relation to the security of the System. Any such direction will provide detail of the action required, a Specified Date by which the action is to be completed, and progress and completion reporting requirements.

2.2.9 The Licensee shall pay for the costs of certification and audits, and the costs of any follow-up actions.

2.3 Governance

2.3.1 In line with its duties and responsibilities, the Authority will ensure the on-going resilience of the System and where any potential or actual security weaknesses are identified, the Authority will determine the necessary and proportionate mitigating steps.

DRAFT