هيئة تنظيم الخدمات العامة

Authority for Public Services Regulation

DRAFT:

ELECTRICITY METERING SYSTEM CYBER SECURITY STANDARD

13 July 2021

Executive Summary

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

- the objective of the standard and the associated regulation;
- the scope and applicability of the standard and regulation;
- the date from which it will be effective;
- definition of terms;
- the Licensee's obligations for:
  - governance
  - risk management
  - establishment and maintenance of a secure system
  - securing data
  - security monitoring
  - security incident response and business continuity planning.

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 standard is presented in the body of this report and should be read along with the technical standards for meters: Technical Standard for Metering Systems and Technical Standard for Prepayment Meters.

Contents

Executive Summary 2

1 Introduction 5

1.1 Objective 5
1.2 Scope 5
1.3 Applicability 5
1.4 Owner 5
1.5 Effective date 5
1.6 Definitions 6

2 Governance 6

2.1 Roles and responsibilities 6
2.2 Information Security Management System 7
2.3 Audit and certification 7

3 Understanding the risk 8

3.1 Risk management 8
3.2 Risk assessment method 8
3.3 Third party and supply chain risk management 9

4 Establish and maintain a secure system 9

4.1 Technical architecture 9
4.2 Security architecture 10
4.3 Access, authentication and personnel vetting 10
4.4 Duty to separate 11
4.5 Asset management 11
4.6 Management of vulnerabilities 12
4.7 Configuration & patch management 12
4.8 Consumer premises equipment 13
4.9 Telecommunications 13
4.10 Central services 14
4.11 Physical security 14

5 Data security 14

5.1 Management of Data 14

5.2 Secure cryptographic processing of data 15

6 Monitoring and detection of security events 16

7 Security incident response and business continuity 16

7.1 Responding to security incidents 17

7.2 Business Continuity Management 17

8 Exceptions 17

1 Introduction

1.1 Objective

1.1.1 The objective of this Standard and the Electricity Metering System Regulation (the Regulation) 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.

1.1.2 This Standard defines the minimum mandatory baseline security requirements for the System by defining the required security outcomes, leaving it to the Licensees to implement measures to fulfil these requirements.

1.1.3 This standard should be read along with the Technical Standard for Metering Systems and Technical Standard for Prepayment Meters, which define the standards for metrology and physical characteristics of the meters.

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) Communications:

- (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).

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

1.3 Applicability

1.3.1 The Regulation and Standard are applicable Licensed Distribution System Operators (Licensee).

1.4 Owner

1.4.1 The owner of this standard is the Regulatory Authority.

1.5 Effective date

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

DRAFT

1.6 Definitions

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

(a) **Anomalous Event** is any event which is not an authorised action or data which is incorrect, either through deliberate manipulation or a System error.

(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.

(d) **End-to-End System** (the System) is comprised of the hardware, software, telecommunications, processes and procedures comprising the elements described in 1.1.3 above.

(e) **Information Security Management System** (ISMS) is the collection of policies, procedures, standards and guidelines which define how risks 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) **Regulation** is the Electricity Metering System Cyber Security Regulation.

(i) **Sector Law** is the law promulgated by Royal Decree (78/2004), as amended.

(j) **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.

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

(l) **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.

(m) **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).

(n) **System** is as defined in 1.6.1 (d) above.

2 Governance

Coordinated management of the security of the System is critical to ensuring that there is an integrated approach to design, implementation, operation and maintenance of the System to meet the objective defined in 1.1 above. Governance needs to be established with each organisation delivery part of the System and across the electricity industry.

2.1 Roles and responsibilities

2.1.1 The Licensee shall identify an ultimate Single Point of Accountability (SPoA) with appropriate knowledge and authority to ensure and demonstrate to the Regulator compliance with the Regulation and Standard.

2.1.2 The Licensee shall define and assign specific security roles and responsibilities for all personnel with access to the System or responsibility for the System operation, support or maintenance.

2.1.3 Personnel shall be:

(a) Informed of their security role and responsibilities; and

DRAFT

(b) Provided with necessary training, procedures and support to ensure they can fulfil their security responsibilities.

2.2 Information Security Management System

2.2.1 The Licensee shall define and establish an Information Security Management System (ISMS) for the system scope as defined in paragraph 1.2 above, which shall include, but is not limited to:

(a) Policies

(b) Procedures

(c) Standards.

2.2.2 The Statement of Applicability shall identify the applicable controls from the International Organisation for Standards ISO 27002:2013 (Information technology – Security techniques – Code of practice for information security controls) and any additional controls required to comply with this Standard.

2.2.3 The ISMS shall:

(a) Comply with the International Organization for Standards ISO 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems); and as amended from time-to-time;

(b) Be approved by the SPoA and the Licensee's CEO, including subsequent changes to the ISMS;

(c) Be communicated to relevant personnel and third parties; and

(d) Be reviewed regularly, at least annually or when significant changes occur.

2.3 Audit and certification

2.3.1 The Licensee shall ensure that the ISMS is:

(a) Certified compliant to ISO 27001:2013 within 12 months of the Effective Date or a Specified Date determined by the Authority;

(b) Certified by a Security Auditor for compliance with ISO 27001:2013; and as amended from time-to-time; and

(c) Audited by a Security Auditor at least annually to ensure continuing compliance and certification.

2.3.2 A copy of each audit report and certificate shall be sent securely to the Authority within 30 days of issue by the Licensee.

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

2.3.4 Licensees shall identify relevant suppliers of services and products that provide any part of the System and must comply with this standard.

2.3.5 Licensees shall conduct assurance that the security of services and products from third party suppliers meets the requirements of the Standard:

(a) By a Specified Date determined by the Authority; and

(b) At least annually thereafter.

2.3.6 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:

(a) Detail of the action required;

(b) A Specified Date by which the action is to be completed; and

(c) Requirements for reporting progress to the Authority, if required.

2.3.7 On receipt of a direction from the Authority, the Licensee shall:

(a) Define a plan to implement the required action; and

(b) Submit the plan by secure communications to the Authority.

DRAFT

3 Understanding the risk

The System will provide a much larger “attack surface” for cyber-attacks with the installation of connected, advanced meters in consumer premises throughout Oman. This increases the cyber security risk to the System with the potential to cause disruption of electricity supply to consumers, enable financial fraud, unauthorised disclosure of consumers’ personal data, and undermine confidence in the electricity sector.
A continuous risk management process to identify, evaluate and treat the risks, and which responds to changes to the risks is essential.

3.1 Risk management

3.1.1 The ISMS shall include a risk management process to ensure:

(a) Cyber security risks to the system are identified and evaluated;

(b) Risks are presented to the Licensee’s Board and senior management following a reassessment as defined in paragraph 0 below; and

(c) Reviewed and accepted by the SPoA and the Licensee’s Board.

3.1.2 The Licensee shall assess risks at least annually and at other times, as appropriate, including but not limited to, changes in:

(a) Security Incidents;

(b) Threat levels;

(c) Known vulnerabilities;

(d) System configuration; and

(e) System upgrades.

3.1.3 The risk assessment results shall be documented and risk treatment defined for each risk:

(a) Approved by the SPoA and the Licensee’s Board, including the acceptance of residual risks; and

(b) Implemented.

3.2 Risk assessment method

3.2.1 A process and method shall be established, maintained and implemented which is aligned to the International Organisation for Standards ISO/IEC 27005:2011 (Information Technology – Security Techniques – Information Security Risk Management) and as amended from time to time, or other suitable and internationally recognised methodology.

3.2.2 The risk assessment method shall enable the assessment of risks related to:

(a) Individual elements of the System;

(b) The end-to-end System;

(c) Security functionality;

(d) Interfaces and connections to other systems; and

(e) Remote access and connectivity to the System.

3.2.3 The risk assessment shall be:

(a) Facilitated by a suitably qualified and experienced person familiar with cyber security risk assessments;

(b) Conducted and maintained by a suitably qualified and experienced team familiar with the risk assessment scope; and

(c) Record the risk assessment team members, date of risk assessment, approved and name of approver(s).

DRAFT

3.3 Third party and supply chain risk management

3.3.1 For all products and services supplied or operated by a third party, based on the risk assessment, the Licensee shall include security requirements in:

(a) Requirements to obtain certification of compliance with relevant standards, such as ISO 27001;

(b) Statement of requirements and specifications;

(c) Procurement documentation and evaluation; and

(d) Contracts, including service level agreements, support and maintenance.

3.3.2 The ISMS shall include a process to manage the risks to the System of any element of the System supplied or operated by a third party, including but not limited to:

(a) Hardware, including meters;

(b) Software;

(c) Telecommunications; and

(d) Services.

3.3.3 Any connections to a third party system for any purpose, including but not limited to, exchange of data and remote support, shall be:

(a) Fully documented, including the technical and security architecture of the connection;

(b) Risk assessed; and

(c) Authorised by the SPoA.

3.3.4 Risks shall be assessed in accordance with the risk assessment method defined in 3.2 above.

3.3.5 The risk management process shall include activities to give assurance that any element supplied or operated by a third party or connection to a third party:

(a) Complies with this Standard; and

(b) Is designed, built, deployed, supported and maintained to ensure its security throughout its lifecycle.

3.3.6 Assurance activities shall be conducted at least annually or in response to changes in risk (2.3.7 above).

4 Establish and maintain a secure system

Clearly defined technical and security architectures are required to ensure that all elements of the System are secured appropriately at the element level and when integrated into the System. In addition to the security of the hardware, software, metering devices and telecommunications, physical and personnel security are also key elements of establishing and maintaining a secure System.

4.1 Technical architecture

4.1.1 The Licensee shall define a technical architecture of the System, which defines the high level design of the System, identifies the elements which comprised the System, the communications and key data flows, and it shall be:

(a) Documented

(b) Approved by the SPoA;

(c) Maintained to reflect any changes;

(d) Clearly marked with an appropriate Information Security Classification; and

(e) Protected from unauthorised disclosure.

4.1.2 The technical architecture shall include, but not be limited to:

(a) Details of all elements and components of the system, including those supplied or operated by third parties;

DRAFT

(b) Logical System diagram of elements and networks, including connections to other systems and remote access; and

(c) Logical network diagram, including connections to other systems and remote access.

4.2 Security architecture

4.2.1 The Licensee shall define a security architecture of the System, which defines the strategies, processes and technologies to secure the System, and it shall be:

(a) Documented;

(b) Approved by the SPoA;

(c) Maintained to reflect any changes;

(d) Clearly marked with an appropriate Information Security Classification; and

(e) Protected from unauthorised disclosure.

4.2.2 The security architecture shall include, but not be limited to, the security:

(a) Framework, including security strategies and architectural layers;

(b) Services, including data flows;

(c) Mechanisms, including physical security;

(d) Products and tools deployed to secure and monitor the System; and

(e) Security operations, management, maintenance and support processes.

4.3 Access, authentication and personnel vetting

4.3.1 The Licensee shall define and maintain a process to manage personnel access to the System and their access privileges shall be established to ensure that only authorised personnel are granted access appropriate to their role. The process shall include:

(a) New personnel joining to grant appropriate access;

(b) Personnel changing role related to the System to ensure access is appropriate to the new role and any access no longer required is removed;

(c) Personnel accessing metering devices using optical ports, should they be enabled (also see 4.11); and

(d) Access is removed for personnel no longer in a role related to the System.

4.3.2 All personnel granted access to the System, together with their level of access, shall be authorised by management.

4.3.3 The list of personnel authorised to access the System and their access privileges shall be reviewed regularly, at least annually by the Licensee to ensure access privileges continue to be appropriate to their role.

4.3.4 The ISMS shall include a policy on the use of passwords, which:

(a) Defines the password length and complexity to be to be a minimum of 8 characters comprised of at least two of upper and lower case letters, numbers and special characters;

(b) Is implemented in all elements of the System where technically possible (see section 8 below for exceptions);

(c) Specifies that passwords will be as strong as possible if it is not technically possible to meet the password specification in 4.3.4 (a) above; and

(d) Requires that passwords are changed at least every 90 days, where technically possible.

4.3.5 Strong authentication (for example, Multi-Factor Authentication) shall be used to authenticate personnel when accessing the System remotely or to conduct activities requiring privileged access.

4.3.6 Personnel authorised to access the System or data within the System, shall hold a level of security clearance appropriate to the role(s) performed by that individual and the data to which they have access. As a

DRAFT

minimum, the identity of personnel shall be confirmed by reference to an officially issued identity document including, but not limited to, passport or Oman identity document.

4.3.7 Personnel authorised to carry out functions requiring a higher level of access privileges or access to consumers' personal data shall be confirmed by the Royal Oman Police as having appropriate security clearance. Functions requiring higher level of access privileges include, but is not limited to:

(a) Changes to the central services elements of the System;

(b) Administrator activities;

(c) Changes to the System or issue of service requests which could interrupt the supply of electricity to the consumer; and

(d) Access to consumers' personal data, including but not limited to financial information.

4.4 Duty to separate

4.4.1 Some elements of the System could have the capability to create and issue commands or service requests to Metering Devices, which could affect the supply of electricity to consumers. Any elements with this capability shall be:

(a) Identified and documented;

(b) Separated from any software or firmware that is installed on the System for any other purpose through:

(i) secure logical separation; or

(ii) physical separation (i.e. separate hardware).

4.4.2 Where two elements forming part of the System are separated in accordance with 4.4.1 above, steps shall be taken to ensure either:

(a) That no person has privileged access to both of those elements of the System; or

(b) To the extent that any person has privileged access to both elements of the System, additional controls are established to ensure the activities of that person cannot be used to Compromise the System.

4.4.3 Should the use of optical ports or other interfaces on a metering device be required, it shall be ensured that access cannot be gained to the wider communications network to which the metering device is connected and personnel can only undertake predefined activities (also see 4.11).

4.5 Asset management

4.5.1 The Licensee shall establish and maintain an inventory of all assets which includes, but is not limited to:

(a) All hardware, software and firmware versions;

(b) Configuration details;

(c) Details of patches applied;

(d) Operational status (e.g. testing, operational, spare, non-operational); and

(e) Product status (e.g. current, supported, obsolescent, obsolete).

4.5.2 The asset inventory shall be updated whenever any part of the System is changed including, but not limited to:

(a) Installation, replacement or removal of metering devices;

(b) Application of patches or changes of version of software or firmware;

(c) Changes in operational status; and

(d) Changes in product status.

4.5.3 The asset inventory shall:

(a) Not be stored on the same infrastructure as the System;

(b) Approved by the SPoA;

DRAFT

(c) Clearly marked with an appropriate Information Security Classification; and

(d) Protected from unauthorised disclosure and modification.

4.6 Management of vulnerabilities

4.6.1 The Licensee shall monitor for notification of vulnerabilities relevant to the System from, for example, suppliers, third parties and open source information.

4.6.2 The Licensee shall conduct vulnerability assessments to identify vulnerabilities within the System:

(a) At least annually;

(b) For any new or materially changed element of the System prior to that element becoming operational; and

(c) In the event of a Security Incident.

4.6.3 Vulnerability assessments shall be conducted by a person suitably qualified and experienced to conduct such assessments.

4.6.4 Where a vulnerability is identified other than by a vulnerability assessment of the System, for example by notification by a third party, the operator of the affected element of the System shall comply with 4.6.5 below.

4.6.5 Upon identification of a vulnerability, the Licensee shall:

(a) Conduct a risk assessment to identify:

(i) the risk the vulnerability presents to the System;

(ii) risk treatment to mitigate the risk, which may include short-term temporary measures to be implemented whilst permanent risk treatment is designed, tested and implemented;

(b) Implement risk treatment as soon as reasonably practicable commensurate with the risk;

(c) For medium or high risk vulnerabilities, the Licensee shall submit a report by secure communications method to the Authority within 72 hours of becoming aware of the vulnerability including, but not limited to:

(i) A description of the vulnerability;

(ii) Estimated potential impact of the vulnerability;

(iii) The risk assessment results; and

(iv) Risk treatment plan;

(d) Wherever it is reasonably practicable to do so, notify the manufacturer of the hardware or device or the developer of the software or firmware (as the case may be), unless they are known to be aware of the vulnerability.

4.7 Configuration & patch management

4.7.1 The Licensee shall establish a management procedure for security related patches and firmware updates, including but not limited to identification, evaluation of applicability and priority, risk assessment of applying or not applying, testing and implementation of patches and firmware updates.

4.7.2 Patches and firmware updates shall be verified to be authentic prior to installation on live systems.

4.7.3 Patches and firmware updates shall be tested prior to application on live systems.

4.7.4 Patches and firmware updates shall usually be applied with involvement and/or approval from the vendor/supplier. However, in some circumstances a decision may be taken to apply patches without the vendor/supplier's approval subject to an appropriate risk assessment and testing/validation process. In all cases, the SPoA shall approve the application of patches.

4.7.5 Firmware updates shall only be applied to metering devices using the security controls specified in this document.

4.7.5 Where a patch or firmware cannot be applied for any reason, alternative compensating controls shall be identified and implemented and an exception shall be requested (see section 8 below).

DRAFT

4.8 Consumer premises equipment

4.8.1 The Licensee shall define and maintain a definition of the security characteristics and requirements for all consumer premises equipment, including but not limited to:

(a) Electricity meters;

(b) Communications hubs; and

(c) Home Display Unit.

4.8.2 The defined security characteristics and requirements shall be based on international best practice. Examples which could be used include:

(a) The UK National Cyber Security Centre "Commercial Product Assurance (CPA) for Electricity Meters"[1]; or

(b) The German Federal Office for Information Security Common Criteria for smart meters[2]; or

(c) The European Protection Profile defined in Common Criteria[3]..

4.8.3 The equipment installed in the consumers' premises including, but not limited to the Electricity meter, Communications Hub and In-home Display Unit shall:

(a) Conform with the Licensee's defined security characteristics and requirements; and

(b) Be tested for conformance by an appropriate independent testing organisation.

4.8.4 The Licensee shall:

(a) Ensure conformance testing is completed prior to deploying consumer premises equipment;

(b) Store conformance testing results in compliance with their Information Security Classification Scheme and Handling Policy; and

(c) Submit the conformance testing results to the Authority, if requested to do so.

4.8.5 If for any reason, the equipment fails to comply with the security requirements, an exception shall:

(a) Be fully documented;

(b) Be risk assessed;

(c) Identify alternative mitigating controls; and

(d) Be submitted to the Authority for approval.

4.9 Telecommunications

4.9.1 The Licensee shall procure telecommunications from companies licensed by the Telecommunications Regulatory Authority to operate telecommunications infrastructure and services in the Sultanate of Oman.

4.9.2 The supplier shall comply with the security standards of the International Organisation for Standards with respect to network security, comprising ISO/IEC 27033-1:2009, ISO/IEC 27033-2:2012 and ISO/IEC 27033-3:2010 (Information Technology – Security Techniques – Network Security), and as amended from time to time.

4.9.3 Third party telecommunications infrastructure and services, which are used to enable system to system and human to system communications, shall be designed, implemented, maintained, and operated to secure the confidentiality, integrity and availability of data transmitted over the network.

---

[1] https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa-security-characteristics

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0095b_pdf.pdf?__blob=publicationFile&v=2
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0073b_pdf.pdf?__blob=publicationFile&v=1

[3] https://www.commoncriteriaportal.org/files/ppfiles/Protection%20Profile%20for%20Smart%20Meter%20Minimum%20Security%20requirements_v1-0.pdf

DRAFT

4.9.4 The telecommunications infrastructure and services shall support a minimum standard of IPv6, or equivalent and as amended from time to time.

4.10 Central services

4.10.1 Central services including, but not limited to, the Head End System, Hardware Security Module Unique Transaction Reference Number generator and Meter Data Management System shall:

(a) Comply with this Standard;

(b) Be tested for compliance by an appropriate independent cyber security assurance organisation.

4.10.2 If for any reason, the central service fails to comply with the Standard, an exemption shall:

(a) Be fully documented;

(b) Be risk assessed;

(c) Identify alternative mitigating controls; and

(d) Be submitted to the Authority for approval.

4.11 Physical security

4.11.1Any elements of the System having the capability to create any commands or service request, which when executed on the metering devices, could interrupt the supply of electricity to the consumer, shall be located, configured, tested, operated and maintained in Oman by personnel who are located in Oman.

4.11.2 Elements of the System to which 4.11.1 above applies, shall be:

(a) Located in a secure location; and

(b) Operated from a secure location.

4.11.3 Physical access controls to the location shall be designed, implemented, operated and maintained to ensure that only authorised personnel have physical access to the System.

4.11.4 Local access using optical ports or other interfaces on metering devices will require authentication and data encryption controls. The minimum security protections shall be compliant with the requirements described in 4.4.3 and 5.2.

4.11.5 It shall be ensured that any permitted local access to a metering device using an optical port, or other interface, does not extend to the wider communications system to which the metering device is connected. Local access activities shall be limited to predefined operational requirements that have been subject to risk assessment

5 Data security

The System is a highly complex system which continuously captures, processes and stores millions of items of data on consumers' electricity consumption, financial transactions, alarms, service requests and more. Compromising the integrity of the data, availability of the data for anything more than a short period of time will undermine the ability to provide accurate and timely consumption and confidence in the billing information. Comprise of the confidentiality of the data will undermine confidence in the System to protect consumers' data. It is important that the Licensees employing Cryptographic techniques for securing data and operations, ensure secure administration and use of key management services and therefore the protection of keys is extremely important.

Key management procedures depend on the underlying cryptographic mechanisms, the intended use of the key and the security policy in use. Key management also includes those functions that are executed in cryptographic devices.

5.1 Management of Data

5.1.1 The Licensee shall define, establish and maintain an Information Security Classification Scheme and Handling Policy.

DRAFT

5.1.2 The Information Security Classification Scheme and Handling Policy shall be applicable to:

(a) Information about the system including, but not limited to:

(i) Governance documentation, minutes of meetings, etc.;

(ii) Technical and security architectures;

(iii) Risk assessments;

(iv) System configurations;

(v) Processes and procedures; and

(vi) Security configuration, monitoring capability, incident response and business continuity plans;

(b) Data captured, transmitted and stored by any element of the System including, but not limited to:

(i) Electricity consumption;

(ii) Service requests to meters;

(iii) Alarms; and

(iv) Consumer data.

5.2 Secure cryptographic processing of data

5.2.1 The Licensee shall define, document, establish and maintain a solution for cryptographic processing of data, management of cryptographic and secret key materials, which:

(a) Establishes the model for key management mechanisms to:

(i) define the concepts of key management used to develop and implement the Public Key Infrastructure (PKI) Architectural Solution;

(ii) specify the characteristics of all the relevant key management services;

(iii) establish general principles on the management of key material during its life cycle; and

(iv) establish the conceptual model for key distribution.

5.2.2 Cryptographic Processing shall only be carried out using FIPS 140-2 Level 3 operated Cryptographic Modules.

5.2.3 The solution shall ensure that management of cryptographic material complies with the security standards of the International Organisation for Standard ISO/IEC 11770-1:2010 (Information technology – Security techniques – Key management – Part 1: Framework), and as amended from time to time.

5.2.4 The solution for the secure management of all secret key material, shall be established, in particular for:

(a) The security of Secret Key Material throughout the whole of its lifecycle:

(i) Generate-Key (key generation);

(ii) Register-Key (key registration);

(iii) Create-Key-Certificate (key certification);

(iv) Distribute-Key (key distribution);

(v) Install-Key (key installation);

(vi) Store-key (key storage);

(vii) Derive-Key (key derivation);

(viii) Archive-Key (key archiving);

(ix) Revoke-Key (key revocation);

(x) Deregister-Key (key deregistration); and

(xi) Destroy-Key (key destruction);

(b) Key Protection mechanisms including:

DRAFT

(i) Protection by cryptographic techniques (for example use of digital signatures for entity authentication);

(ii) Protection by non-cryptographic techniques (for example timestamp to restrict the use of keys to certain valid time periods);

(iii) Protection by physical means (for example a FIPS 140-2 Level 3 operated cryptographic device within a secure system to protect the keying material it uses against the threats of modification, deletion and, except for public keys, disclosure. The device would then provide a secure area for key storage, key use and cryptographic algorithm implementation.); and

(iv) Protection by organisational means (for example establishing key hierarchy, documented but restricted key custodianships, robust privilege access control to all cryptography management devices and documents).

(c) Registration Authority policy and procedures documenting the manner in which secret key material will be registered, ordered, generated, labelled, distributed, installed, superseded and renewed; and

(d) the verifiable destruction of secret key material.

6 Monitoring and detection of security events

6.1 Although the security of the System may be designed and implemented to meet the standard and provide a good level of security, it is essential to continuously monitor all elements of the system for any anomalies to provide early warning of any incorrect functioning of the System, unauthorised access or manipulation of data.

6.2 The Licensee shall establish, operate and maintain the capability to detect Anomalous Events within the System, including but not limited to security events, system messages, unusual service requests including remote disconnects, alerts and alarms:

(a) Whether deliberate, accidental or caused by a System error; and

(b) Regardless of whether the System generates an error message, alert or alarm.

6.3 Anomalous Events shall be monitored and assessed by suitably qualified and experienced person(s) to identify appropriate remedial action(s), which may include triggering security incident response plans.

6.4 Security event data including, but not limited to messages, alerts, alarms, logs and Security Information and Event Management system databases, shall be stored separately from the System to protect its integrity.

6.5 Arrangements for storage of security event data shall comply with the International Organisation for Standards ISO 27040:2015 (Information technology – Security techniques – Storage security), and as amended from time to time, such as to prevent the alteration or destruction of security event and related data.

6.6 The content of service requests shall be inspected in real-time to ensure that unauthorised or invalid requests, such as service disconnection, are not sent to metering devices and are reported.

6.7 The number of each type of service request within a defined period shall be monitored to identify unusual levels of requests. Unusually large or small numbers of requests shall be investigated to identify the cause and, if required, remedial action implemented.

7 Security incident response and business continuity

Despite the best efforts to make and keep the System secure, there is the potential for cyber security incidents to occur. If such an event occurs, having prepared for this by having incident response and business continuity plans developed, exercised and tested will enable rapid and effective response, which will minimise the impact of incidents.

DRAFT

7.1 Responding to security incidents

7.1.1 The Licensee shall establish an Incident Response plan, which complies with the International Organisation for Standards ISO/IEC 27035:2011 (Information Technology – Security Techniques – Information Security Incident Management), and as amended from time to time.

7.1.2 Reasonable steps shall be taken to ensure that:

(a) The System is capable of identifying any deviation from the expected configuration; and

(b) Any identified deviation is corrected.

7.1.3 Reasonable steps shall be taken to:

(a) Ensure that the System is capable of detecting any unauthorised software that has been installed or executed on it and any unauthorised attempt to install or execute software;

(b) Prevent the installation or execution of unauthorised software; and

(c) Take appropriate action if any unauthorised software has been installed or executed.

7.1.4 There shall be the capability to:

(a) Ensure that the System records all attempts to access resources or data in the system;

(b) Ensure that the System detects any attempt by any person to access resources or data that is not authorised to do so; and

(c) Take reasonable steps to ensure that the Systems prevents any such attempt at unauthorised access.

7.1.5 Security incidents and the resulting actions shall be:

(a) Documented, including, but not limited to root causes and remedial actions taken to prevent future similar incidents;

(b) Reported by secure communications methods to the Authority within 24 hours of becoming aware of the incident.

7.2 Business Continuity Management

7.2.1 The Licensee shall establish a Business Continuity Management Plan, which complies with the International Organisation for Standards ISO/IEC 22301:2012 (Societal Security – Business Continuity Management Systems – Requirements) and ISO/IEC 27031:2011 (Information Technology – Security Techniques – Guidelines for Information and Communications Technology Readiness for Business Continuity), as amended from time to time.

8 Exceptions

8.1 If it is not possible to comply with any part of this Standard, any controls or procedures in the ISMS, or any directive issued by the Authority, in whole or in part, the Licensee shall raise an exception, which shall:

(a) Fully document any area of non-compliance, including the reasons why compliance is not possible;

(b) Assess the impact and risk of non-compliance;

(c) Identify compensating alternative controls;

(d) Be approved by the SPoA;

(e) Communicated to the Licensee's Board; and

(f) Submitted by secure communications to the Authority for approval.

8.2 On receipt of approval for the exception from the Authority, the compensating alternative controls shall be implemented as soon as practicable.

8.3 If there is a likelihood of a cyber incident occurring, for example if there is a specific threat or known to be active exploitation of a vulnerability:

DRAFT

(a) Compensating alternative controls should be implemented immediately without waiting for the approval from the Authority

(b) The Authority shall be notified by secure communications and approval to be obtained.

DRAFT