CONDITION 8. SECURITY CONTROLS FOR THE AUTHORISED BUSINESS

Introduction

8.1 This condition requires the Licensee to install, operate, and maintain adequate and proportionate security controls that are designed to protect the integrity of the physical, organisational, and information assets of the Authorised Business.

8.2 The requirements of this condition are without prejudice to the obligations imposed on the Licensee by**:**

(a) Condition 7 (General controls for the Authorised Business) in respect of corporate governance, internal control, and risk management;

(b) Condition 10 (Protection of Confidential Information) in respect of the duty to prevent unauthorised disclosure of Confidential Information; and

(c) such requirements or other provisions of the SEC and / or REC as may apply in respect of security controls relating to the conduct of the Authorised Business.

Part A: Requirements for Licensee's control of physical security

8.3 The Licensee must at all times have in place a system of controls that is designed to ensure the security of all equipment, networks, processes, procedures, and data used in or for the purposes of carrying on the Authorised Business so as to minimise opportunities for theft, fraud, or other unauthorised interference or misuse that whether directly or indirectly could cause any interruption or cessation of Services.

8.4 In particular, the system of controls to which paragraph 8.3 refers must include measures designed to ensure that**:**

(a) equipment transported, installed, or operated by the Licensee for the purposes of the Authorised Business is protected against unauthorised access;

(b) the supply, repair, and maintenance of such equipment, and the supply of spare parts for it, are at all times under the control of the Licensee;

(c) all premises used for or in connection with the conduct of the Authorised Business are physically secured and monitored;

(d) equipment and data that are no longer required for any of the purposes of the Authorised Business are securely disposed of or deleted; and

~~(e) data processed by the Licensee for the purposes of the Authorised Business is not held outside the European Economic Area; and~~

~~(f)~~(e) where data is to be transferred, it is transferred in a secure manner.

Part B: Requirements for Licensee's control of organisational security

8.5 The Licensee must verify (by such means as may be appropriate in each case) the backgrounds of its existing and all new personnel engaged in or for the purposes of carrying on the Authorised Business.

8.6 Without prejudice to its obligations under Part E below, the Licensee's duty under paragraph 8.5 includes a requirement to take all appropriate steps within its power to ensure that any agents and contractors of the Licensee (including, in particular, its External Service Providers) establish and maintain arrangements that are equivalent in their effect to those established and maintained by the Licensee for the purposes of that paragraph.

8.7 The Licensee must have in place an appropriate framework for security management that provides for an appropriately qualified Chief Information Security Officer to be directly responsible to the Licensee's board of directors for ensuring that**:**

(a) the Licensee's security policies are communicated to all of its staff;

(b) training that is tailored to the security roles and responsibilities of different staff within the Licensee's organisation is provided on a regular basis;

(c) each person engaged in or for the purposes of the Authorised Business is (and remains) (i) a fit and proper person to be so engaged, and (ii) suitably qualified and appropriately trained to be so engaged; and

(d) the Licensee is at all times compliant with the requirements of this condition and (to the extent applicable) of the SEC and / or REC with respect to security controls for the Authorised Business.

8.8 This paragraph applies if, in premises that are occupied by (i) the Licensee or an External Service Provider and (ii) some other person, there is any area that must be kept secure in order to maintain the security of the Authorised Business.

8.9 Where paragraph 8.8 applies, the Licensee must ensure that**:**

(a) the area to which that paragraph refers (which may be the whole or any part of the area occupied by the Licensee or an External Services Provider within the premises in question) is designated as a Secure Area; and

(b) an appropriate level of security in relation to the Secure Area is maintained (in particular, by ensuring that no person gains access to such area unless it is a person whose name is on a register maintained by the Licensee or the External Service Provider for that purpose, or who is supervised by such a person).

Part C: Requirements for Licensee's control of information security

8.10 The Licensee must, within 12 months after it first provides Core Communication Services under or pursuant to the SEC, hold appropriate certification by a body that is accredited by the United Kingdom Accreditation Service in relation to the following standards of the International Organisation for Standards ("ISO") with respect to the

resilience, reliability, and security of information assets, processes, and systems used for the purposes of carrying on the Authorised Business**:**

(a) ISO/IEC 27001**:**2005 (under the title of *Information Technology – Security Techniques – Information Security Management Systems*); and

(b) any equivalent standard of the ISO that updates or replaces that standard.

Part D: Requirement to maintain a Register of Security Incidents

8.11 The Licensee must**:**

(a) maintain a register of every incident (as may be defined in accordance with such provisions of the SEC as are applicable) arising from a failure (whether actual or apparent) or an absence of any of the security controls established, operated, and maintained by the Licensee pursuant to this condition ("the Register of Security Incidents");

(b) record each such incident in the Register of Security Incidents immediately upon becoming aware of it;

(c) immediately inform such body as is required by the provisions of the SEC to be so informed of the incident as soon as the Licensee has become aware of it; and

(d) within such timescale as is specified by the Authority, provide the Authority with a report that details**:**

(i) the nature, cause, and impact (or likely impact) of the incident,

(ii) the action taken by the Licensee to remedy or minimise the immediate or expected consequences of the incident, and

(iii) the action taken (or proposed to be taken) by the Licensee to ensure that the incident does not recur, or that the risk of recurrence is minimised.

8.12 The Licensee must also**:**

(a) make the Register of Security Incidents available to the Authority for its inspection at all times; and

(b) provide the Authority with a copy of the Register of Security Incidents on the expiry or any revocation of this Licence, or where and to the extent applicable, pursuant to direction by the Authority under Condition 15.6.

Part E: Requirements in respect of the Licensee's contracts

8.13 The Licensee must not enter into any contractual arrangement with any person (including, in particular, any External Service Provider) that does not contain appropriate provisions requiring such steps to be taken as may be necessary to facilitate the Licensee's fulfilment of its obligations under this condition and under or pursuant to the SEC in respect of the ongoing security of its physical, organisational,

and information assets.

8.14 The provisions mentioned in paragraph 8.13 include, in relation to the expiry or any termination of an External Service Provider Contract**:**

(a) requirements for an External Service Provider to return or provide to the Licensee any equipment or other physical or organisational assets and any information assets that are essential to the ongoing secure conduct of the Authorised Business; and

(b) requirements for the Licensee to revoke any security credentials that are held by the External Services Provider pursuant to that contract.

Part F: Legal and operational location of the Licensee

8.15 The Licensee must at all times**:**

(a) remain a company that is incorporated in the European Economic Area;

(b) procure the SMKI Service (within the meaning that is given to that term in Schedule 5 to this Licence), except to such extent as is otherwise permitted by the SEC, from Relevant Service Capability the provision and management of which are carried on within the United Kingdom; and

(c) ensure that all sites and systems that the Licensee relies upon to detect and prevent events that**:**

(i) appear to be anomalous; and

(ii) may have the potential to impact on the Supply of Energy to Energy Consumers,

are configured, operated, and maintained within the United Kingdom.

Part G: Interpretation

8.16 For the purposes of this condition**:**

Chief Information Security Officer means the person having the duties set out at paragraph 8.8 and who is qualified as a senior security manager.

Register of Security Incidents has the meaning that is given to that term in paragraph 8.11(a).

Secure Area has the meaning that is given to that term in paragraph 8.9(a).

SECTION I: DATA PRIVACY

I1 DATA PROTECTION AND ACCESS TO DATA

Without Prejudice

I1.1 The obligations of the DCC and each User under this Section I1 are without prejudice to any other obligations they each may have under the Data Protection Legislation and other Relevant Instruments, including any such obligations they each may have concerning Processing of Personal Data.

User Obligations

Consumption Data

I1.2 Each User undertakes that it will not request, in respect of a Smart Metering System, a Communication Service or Local Command Service that will result in it obtaining Consumption Data, unless:

(a) the User has the Appropriate Permission in respect of that Smart Metering System; and

(b) (where that User is not the Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor or Gas Transporter for that Smart Metering System) the User has, at the point of obtaining Appropriate Permission and at such intervals as are reasonably determined appropriate by the User for the purposes of ensuring that the Energy Consumer is regularly updated of such matters, notified the Energy Consumer in writing of:

(i) the time periods (by reference to length) in respect of which the User obtains or may obtain Consumption Data;

(ii) the purposes for which that Consumption Data is, or may be, used by the User; and

(iii) the Energy Consumer's right to object or withdraw consent (as the case may be) to the User obtaining or using that Consumption Data, and the process by which the Energy Consumer may object or withdraw consent.

Service Requests

I1.3 Each User undertakes that it will not send either a 'Join Service' or 'Unjoin Service' Service Request (respectively to join a Type 2 Device to, or unjoin it from, any Smart Meter or Device Associated with a Smart Meter) unless:

(a) the User is the Responsible Supplier for the Smart Meter or Associated Device to which the Service Request is sent, and sends that Service Request for the purpose of complying with an obligation under its Energy Supply Licence; or

(b) the Energy Consumer at the premises at which the Smart Meter is located has given the User Unambiguous Consent, which has not been withdrawn, to (as the case may be):

(i) join that Type 2 Device to the Smart Meter or Associated Device, and the User has clearly informed the Energy Consumer before obtaining such Unambiguous Consent that a consequence of joining the Type 2 Device may be that Data relating to the Energy Consumer will be shared with third parties; or

(ii) unjoin it from the Smart Meter or Associated Device, save that the Responsible Supplier for a Smart Metering System at the premises need not obtain such Unambiguous Consent where it has reasonable grounds to believe that the Type 2 Device has Compromised or is likely to Compromise any Device forming part of that Smart Metering System (and the Responsible Supplier shall, where it unjoins a Type 2 Device in such circumstances, take all reasonable steps to inform the Energy Consumer that it has done so).

Access to Records

I1.4 Each User undertakes that it will not access (pursuant to Section H8.16) or request (pursuant to Section H8.17) the information described in Section H8.16(c), unless:

(a) the Energy Consumer at the premises at which the relevant Smart Meter is located has given the User Unambiguous Consent to do so and such consent has not been withdrawn; and

(b) the information is accessed solely for the purpose of its provision to that Energy Consumer.

Good Industry Practice

I1.5 Each User shall put in place and maintain arrangements designed in accordance with Good Industry Practice to ensure that each person from whom it has obtained consent pursuant to Section I1.2 to I1.4 is the Energy Consumer.

Processing of Personal Data by the DCC

I1.6 It is acknowledged that, in providing the Services to a User, the DCC may act in the capacity of 'Data Processor' on behalf of that User in respect of the Personal Data for which that User is the 'Data Controller'.

I1.6A The Personal Data which the DCC will Process as a Data Processor on behalf of Users will relate to Energy Consumers, and will include Personal Data which is included within messages sent and received by the DCC via the DCC User Interface or the Self-Service Interface, and/or which is included within messages sent or received by the DCC to or from Communications Hubs. The nature of such Personal Data will be that which is required or permitted to be included in such messages as described in this Code. The full description of the subject matter, the nature and purpose of the processing, and the type of personal data is as described by this Code as a whole.

I1.7 The DCC undertakes for the benefit of each User in respect of the Personal Data for which that User is the 'Data Controller' to:

(a) only Process that Personal Data for the purposes permitted by the DCC Licence and this Code (subject to paragraph (d) below);

(b) only Process that Personal Data for so long as it is required to do so by the DCC Licence and this Code;

(c) undertake the Processing of that Personal Data in accordance with the DCC Licence and this Code, (to the extent consistent with the DCC Licence and this Code) on the documented instructions of the User, and (subject to the foregoing requirements of this Section I1.7(c)) not in a manner that the DCC knows (or should reasonably know) is likely to cause the User to breach its obligations under the Data Protection Legislation (subject to paragraph (d) below);

(d) if the DCC is aware that, or is of the opinion that, any requirement of paragraph (a) (b) or (c) above infringes the Data Protection Legislation, the DCC shall immediately inform the User of this giving details of the infringement or potential infringement (unless the DCC is prohibited from doing so by any of its other obligations under Laws and Directives);

(e) ensure that the DCC's personnel who are authorised to Process Personal Data are under enforceable obligations of confidentiality and are required only to Process that Personal Data in accordance with the DCC's obligations under the DCC Licence and this Code;

(f) having regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, implement appropriate technical and organisational measures to protect that Personal Data in particular from accidental or unlawful loss, destruction, alteration or unauthorised disclosure of, or access to personal data transmitted, stored or otherwise Processed (such measures to at least be in accordance with Good Industry Practice and the requirements of Section G (Security));

~~(g) not transfer or Process that Personal Data outside the European Economic Area;~~

~~(h)~~(g) taking into account the nature of the Processing assist the User with its obligations to comply with Data Subjects' requests and Data Subjects' rights under the Data Protection Legislation in respect of that Personal Data through,

insofar as is possible, the use of appropriate technical and organisational measures;

~~(i)~~(h) taking into account the nature of the Processing and the information available to the DCC, assist the User in ensuring compliance with the User's obligations in Articles 32-36 of the General Data Protection Regulation (or its national equivalent), including:

(i) notifying the User without undue delay if the DCC becomes aware of a breach of the Data Protection Legislation in relation to the Personal Data (including in the event of unauthorised access to such Personal Data); and

(ii) providing full details of the relevant breach where caused by the DCC or any Sub-Processor without undue delay or, where necessary, in phases but always without further undue delay;

~~(j)~~(i) provide reasonable assistance to the User in complying with any enquiry made, or investigation or assessment initiated, by the Information Commissioner or any other Competent Authority in respect of the Processing of that Personal Data pursuant to this Code;

~~(k)~~(j) promptly notify the User in the event that the DCC Processes any of that Personal Data otherwise than in accordance with this Code (including in the event of unauthorised access to such Personal Data);

~~(l)~~(k) notify the User of any complaint relating to the DCC's obligations under the Data Protection Legislation in respect of the Processing of that Personal Data pursuant to this Code;

~~(m)~~(l) after the end of the provision of the Services to which the Processing of that Personal Data relates, at the written election of the User, either securely destroy the Personal Data or return it to the User together with all copies (save to the extent that the DCC is required by Laws and Directives to retain a copy of the Personal Data); and

~~(n)~~(m) permit the Independent Privacy Auditor (on the instruction of SECCo on behalf of Users collectively), on giving reasonable prior notice of its intention to audit, to audit the DCC's compliance with this Section I1.7 during normal business hours, and shall make available to the Independent Privacy Auditor all information, systems and staff reasonably necessary for the Independent Privacy Auditor to conduct such audit. The number of audits shall be limited to no more than once in every twelve (12) calendar month period unless more frequent audits are required under the Data Protection Legislation or the Panel has grounds to suspect there has or is likely to be a breach of the Data Protection Legislation. Where practicable, DCC shall be provided with an opportunity to comment upon the scope of an audit in advance and any audit shall be carried out in such a way that interruption to DCC's operations is minimised as far as is reasonably possible.

DCC's Sub-Processors

I1.8 The DCC shall ensure that its Sub-Processor(s) are subject to written contractual obligations in respect of the Processing of Personal Data which are at least equivalent to the obligations imposed on the DCC under the DCC Licence and this Code, including obligations which provide sufficient guarantees from the Sub-Processor that the Processing meets the requirements stated at any time in the Data Protection Legislation.

I1.9 Each User hereby gives its general authorisation to the DCC to engage Sub-Processor(s) who are appointed in accordance with the DCC Licence and does not object to the engagement by the DCC of any Sub-Processor provided that in engaging the Sub-Processor the DCC complies with the DCC Licence and this Code and publishes on its Website the identity of the Sub-Processor(s) from time to time. Each User hereby consents to Processing by each such Sub-Processor who is appointed in accordance with the DCC Licence and this Code.

Records

I1.10 The DCC and each User will each maintain in accordance with Good Industry Practice all such records and other information as is necessary to enable the DCC and each such

User to demonstrate that it is complying with its respective obligations under Sections I1.2 to I1.9.

I1.11 The DCC shall make available to each User all information reasonably necessary to demonstrate compliance by the DCC with Sections I1.6 to I1.9, but only insofar as such information relates to the Personal Data for which that User is the Data Controller.

General Compliance with Data Protection Legislation

I1.12 Each of the DCC, SECCo, and each User undertakes to comply with its obligations under the Data Protection Legislation in respect of Personal Data they Process as a Data Controller or Data Processor pursuant to this Code.

Permission for Gas Supplier to Store Data on shared SMETS1 Installation

I1.13 In the case of a SMETS1 GSME which forms part of the same SMETS1 Installation as a SMETS1 ESME, and where the Gas Supplier for the SMETS1 GSME is a different person to the Import Supplier for the SMETS1 ESME, the Import Supplier hereby agrees to permit the Gas Supplier to store Data on the SMETS1 GPF which forms part of that SMETS1 Installation in the manner envisioned by SMETS1.