Smart Energy Code

Section G: Security

SEC Section G provisions concern:

- SEC Parties
- Data and Communications Company
- Registered Supplier Agents
- SEC Panel
- The Authority

What does Section G cover?

Section G details the **security arrangements** which are designed under a principle that there must be no single point of vulnerability. This guide provides an overview of the arrangements set out within this section.

General Obligations

There are a number of general obligations set out within Section G1 that the rest of Section G must be read in accordance with. These cover:

- **Compliance with Standards –** where the DCC or User is required to ensure compliance with any standard, procedure or guideline issued by a third party, and the standards are updated or replaced, then the DCC or User must comply with the updated standard from a date specified by the Panel.
- **Obligations on Users –** where an obligation is placed on a User, it shall apply separately to each User Role performed by that User (including Registration Data Providers which must be treated separately to Network Operators).
- **Export Suppliers and Registered Supplier Agents –** there are a number of exclusions on obligations set out within Section G for Export Suppliers and Registered Supplier Agents.
- **Disputes –** Any dispute regarding the compliance of a User with the obligations set out within Sections G3 – G6 may be referred to the Panel for determination. If a Party disagrees with a Panel determination, then the matter may be referred to the Authority in accordance with Section M7 (Dispute Resolution).

Security Overview

The SEC classes DCC and User security obligations into three categories:

1. **System Security** – requires ensuring the overall security of systems with protective monitoring of events and any deviations from steady state operation.
2. **Organisational Security** – requires ensuring that personnel able to access systems are granted an appropriate level of access, ensuring that users with high levels of access are appropriately cleared.
3. **Information Security** – requires establishing Information Security Management Systems which shall also comply with recognised International Standards.

In addition to the three categories above, all of which are described in greater detail elsewhere in this guide, there are also obligations relating to the assurance and enforcement of security measures.

Each User has SEC responsibilities for the identification and management of the risk of Compromise, which shall comply with the ISO27005 standard, or equivalent.

System Security: DCC Obligations

To ensure security of the Total System, the SEC places a number of obligations on the DCC. Furthermore, some of these security obligations are subject to specific standards, such as **Protective Monitoring** in accordance with the **CESG Good Practice Guide** and recording activity on the DCC Systems in accordance with **BS 10008:2008**.

The DCC has some additional obligations related to its role, which include:

- the ability to detect and react to unauthorised connection attempts;
- the ability for the Total System to detect alterations from expected configuration;
- the network is limited must only allow connections over specific ports and protocols;
- the Total System must be able to detect Denial of Service Events and must take best endeavours to ensure that the system is not comprised;
- having an annual audit of their systems, performed by a CESG CHECK qualified service provider;
- ensuring the security and data integrity of SM WAN communications;
- notifying security vulnerabilities in the Parse & Correlate Software; and
- ensuring Cryptographic Credential Tokens, Smart Card Tokens and File Sharing Software that it provides to any person in accordance with the SEC is appropriately secure.

Further detail on the DCC's security obligations can be found throughout Section G, particularly **G2.**

System Security: User Obligations

Section **G3** specifies the system security measures which Users are expected to take, including a duty to detect and respond to unauthorised activities. All Users are required to take security into account at all stages of its **System Development Lifecycle**.

Suppliers are further required to have vulnerability assessments carried out by an accredited body at least annually.

SEC places each User under reasonable endeavours to separate its security software or firmware from other components of its User System.

The physical location of components of a User System for specified cases is constrained to the UK.

Suppliers are also required to detect Anomalous Events and a material security vulnerability in a Smart Metering System.

Organisational Security

Users and the DCC are required to regulate who has physical access to their User Systems and the DCC Total System respectively. Section **G4** explains how this regulation should be implemented.

Security clearance, which must be reviewed annually, must be appropriate to the role an individual is performing. Whilst not required of all Users, those with a high level of access as contemplated in SEC **G4.2 and G4.6** must undergo screening consistent with the appropriate British Standard (**BS 7858:2012**).

Information Security

Part of the Security obligations set out within Section **G5** include the creation of an **Information Security Management System** (User ISMS) by the DCC and each User which sets out the approach to:

- complying with the System and Organisation security obligations;
- meeting the ISO ISO/IEC 27001:2013 or equivalent standard; and
- operating appropriate security controls.

SEC Section G5.19 – G5.24 sets out requirements that the User ISMS must include, such as:

- an information security policy;
- access control measures;
- physical and information asset registers;
- arrangements for information, personnel and physical/environmental security;
- management of information security incidents in accordance with standard ISO/IEC27035; and
- management of the User's Secret Key Material.

The breadth of these obligations is expected to be proportionate to the role the User plays in protecting the end-to-end smart metering security architecture.

The contents of each User's ISMS will be unique. The User ISMS must be tailored to the specific nature and requirements of each User, whilst also being sufficiently robust to mitigate the risk of security vulnerabilities.

Shared Resources

Users are required to inform the Security Sub-Committee if they intend to make use of Shared Resources. They must provide details of any third party providers involved and information on the total number of Devices involved.

Parties are expected to incorporate the use of Shared Resources into their UISMS and adjust their security controls proportionately.

Security Sub-Committee

The Panel will establish the Security Sub-Committee (SSC) to oversee, review and advise on SEC security arrangements. The SSC duties include overseeing the Security Controls Framework and assurance, and maintaining the Security Architecture and annual Risk Assessment.

The SSC will meet on a regular basis to discuss and review security issues across all aspects of the smart metering arrangements, seeking the advice of the Alt HAN Forum where necessary.

For further information on the SSC please see the SSC page on the SEC Website.

Anomaly Detection Thresholds

For the purpose of detecting anomalous activity and events, Users and the DCC must set **Anomaly Detection Thresholds** set at a level designed to ensure an effective means of Compromise to systems. These Anomaly Detection Thresholds must be kept under review to ensure they remain appropriate.

Users and the DCC must comply with the **Threshold Anomaly Detection Procedures**. This SEC Subsidiary Document sets out:

- Any guidance for Users in setting Anomaly Detection Thresholds;
- Any actions to be taken when an Anomaly Detection Threshold has been exceeded, including the quarantining of messages; and
- The means by which thresholds will be notified to the DCC and notifications on the quarantining of messages.

The DCC must notify the Security Sub-Committee (SSC) of any thresholds that they set and that are set by Users.

The DCC will also consult the SSC on any thresholds that they set.

User Security Assurance

The SEC Panel must appoint a **User Independent Security Assurance Service Provider** (UISASP) to assess all User's security arrangements. A Security Controls Framework will be developed by the Security Sub-Committee; which will define the methodology upon which security assurance assessments will be based.

Whilst the specifics of an assessment will vary depending upon the nature of the User, Security Assessments will follow a 3 year rolling cycle and fall into one of the categories below:

1. **Full User Security Assessment** – this involves a full assessment of a User's System, Organisation and Information Security measures by the User CIO.
2. **Verification User Security Assessment** – a less exhaustive assessment than the Full User Security Assessment, comprising the User CIO's review of any material changes to the security risk of Information Security measures since the User's last Full Assessment.
3. **User Security Self-Assessment** – the User is responsible for performing their own assessment of their Information Security Measures, with the outcome being reviewed by the User CIO.
4. **Follow-up Security Assessment** – in some circumstances the User CIO may decide to perform an assessment of any actions agreed as a result of a User Security Self-Assessment.

Users are bound by the SEC to cooperate in all Assessments. The frequency of these assessments is dependent upon the size of the Party being assessed, with larger Parties being assessed more frequently. Charges for these assessments, which will be payable by the Party being assured, are being determined by Panel and will be notified in due course.

Further information on the Security Assessment process can be found on the Security Assessment page on the SEC website.

DCC Security Assurance

Section **G9** sets out the **DCC Independent Security Assurance Arrangements** which include appointing a DCC Independent Security Assurance Service Provider. The service provider will provide security assurance services which include performing SOC2 assessments of the DCC and providing a DCC Security Assessment Report to the Panel and the Security Sub-Committee.

The SOC2 assessments will cover the security risk assessments undertaken by the DCC, an assessment of the effectiveness and proportionality of the security controls and the DCC's compliance with the security requirements set out within the Code, the DCC Licence and any other specified requirements.

In the event that an Event of Default has occurred in relation to any of the DCC's obligations set out within Section **G9.2(c),** the Panel may refer the matter to the Security Sub-Committee for investigation and advice.

Disclaimer

These guides are intended to provide a simple overview of the SEC and any supporting or related arrangements and do not replace or supersede the SEC or these related arrangements in any way. The author does not accept any liability for error, omission or inconsistency with the SEC.

Contact Us:

For all enquires or further advice, please contact SECAS at:

W: smartenergycodecompany.co.uk

T: 020 7090 7755

E: secas@gemserv.com