Data Communications Company

Compliance Statement

May 2022

Version: 1.7
Date: May 2022
Author: Head of Information Governance and Data Protection
Classification: DCC Public

Table of Contents

1. Document control 2
2. Purpose 3
3. Management of Confidential Information 4
4. Information Management Systems 5

1. Document control

Revision history

Revision date	Summary of changes	Changes marked	Version number
20/12/2013	First published	No	1.0
10/05/2016	Minor wording and template update	No	1.1
8/10/2019	Update to reflect new approach to Confidential Information	No	1.2
30/10/2019	Updated based on CISO review	No	1.3
20/11/2019	Updated based on Business Assurance Manager review	No	1.4
28/08/2020	Updated to reflect broadening scope of Confidential Information and added into new DCC document template	Text change – Yes Formatting – No	1.5
10/06/2021	2021 annual review Additional content added to reflect working conditions under COVID-19. Additional minor updated to body text	Yes	1.6
24/05/2022	Numbering issues addressed	Only formatting no other changes made.	1.7

Date of next review: June 2023

2. Purpose

2.1 Smart DCC Ltd ("Smart DCC" is the holder of Smart Meter Communication Licence granted by the Secretary of State under sections 7AB (2) and (4) Gas Act 1986 and section 6 (1A) and (1C) of the Electricity Act 1989 (together "the Licence") and having a Licence Commencement Date of 23 September 2013.

2.2 This is the Compliance Statement (the "Statement") as required by Condition 10 of the Licence setting out Smart DCC's managerial and operational practices, systems and procedures to ensure that it complies with the General Prohibition pertaining to the protection of Confidential Information.

2.3 This Statement sets out the practices in place to ensure that Confidential Information is only used for the purposes of the Smart DCC business and is not used for any other interest including that from other areas of Capita plc, or any other organisation or person.

2.4 It is the responsibility of the Smart DCC to ensure that any Affiliate or Related Undertaking of Smart DCC, and any agent, consultant, or contractor of Smart DCC are also governed by the conditions of this Statement.

2.5 This Statement may only be revised with the approval of the Gas and Electricity Markets Authority that is established under section 1 of the Utilities Act 2000 (the "Authority").

2.6 Smart DCC is a wholly owned subsidiary of Capita plc and is regulated by the Authority.

2.7 Smart DCC has been granted the Licence to establish and manage the smart metering communications infrastructure which is governed by the Smart Energy Code and those documents referenced therein.

2.8 Smart DCC is responsible for the establishment and enduring governance of the smart metering communications infrastructure and during its term shall collect and create information in order to provide these services. Such information consists of design documentation, business process models, audit information, service management data, service user contact details, billing data and management information.

2.9 Smart DCC takes all appropriate steps within its power to ensure compliance with the terms of this Statement.

2.10 Words or expressions that are not specifically defined in this document shall, where applicable, have the meaning given to them in the Licence.

3. Management of Confidential Information

3.1 Confidential Information is defined within the Licence as "information that is provided to the Licensee (whether directly or indirectly) by any person in connection with the Authorised Business of the Licensee, including information that is provided under or pursuant to the Smart Energy Code, Retail Energy Code or the provisions of any External Service Provider Contract to which the Licensee is a party (and includes any personal data and sensitive personal data within the meaning of the Data Protection Act 1998)"

3.2 The Data Protection Act 1998 remains as a reference in the Licence but has since been replaced by the Data Protection Act 2018 and the UK General Data Protection Regulation. Smart DCC therefore takes as its reference the current data protection legislation for the definition of personal data.

3.3 Provisions relating to DCC's management of Confidential Information in the Licence are set out in Condition 8 Part C of the Licence (which requires DCC to hold appropriate certification relating to information security, and in Condition 10 of the Licence relating to the protection of Confidential Information.

3.4 The smart metering communications infrastructure has been designed such that all consumption data sent between service users and smart meters is encrypted and is therefore not visible to Smart DCC.

3.5 A register of Confidential Information assets is maintained which identifies the purpose of the information asset and formally assigns ownership of each to an information asset owner (a member of the Smart DCC executive committee). The register captures all important information assets such as system documentation, database content and contracts.

3.6 Those members of the Smart DCC Executive Committee who have been assigned as the authorised processors of Confidential Information are formally included within information management processes in order that appropriate authorisation is provided for all data being accessed, disclosed or changed.

3.7 Requests for the disclosure of, or access to, Confidential Information are recorded using the log maintained by the Commercial Director's team and may be validated if justified appropriately. Only then may Confidential Information be shared with DCC customers or service providers, and only where a valid business purpose for receiving the Confidential Information has been identified. Internally the Business Improvement and Audit team will ensure compliance with this process, as will the Independent Compliance Officer following requirements within Licence Condition 12 and overall compliance with Chapter 3 of the Licence. Other auditors may access Confidential Information through signed contracts which contain non-disclosure agreements.

3.8 Confidential information is managed in accordance with the following principles:

- Data is only retained for periods necessitated by the purposes of its use
- Data is stored in as few places possible and for as short a time as possible
- Data is disclosed only to those who need to have access for identified business purposes

3.9 Physical data is:

- Stored in fixed lockable containers
- Transferred using secure methods (e.g. a secure courier)
- Shredded or otherwise destroyed when no longer required

3.10 Electronic data is:

- Protected using user authentication and defined access controls
- Encrypted when being transmitted over secure communications channels
- Securely deleted when no longer required

3.11 All Smart DCC employees have specific obligations towards the protection of information within their terms and conditions of employment and disciplinary processes shall be used should those conditions not be met.

3.12 All Smart DCC employees are provided with mandatory annual training on topics including cyber and information security, fraud, data privacy and Smart DCC's Regulatory obligations. For those Smart DCC employees who are provided access to Confidential Information, additional guidance is provided on their responsibilities towards the correct handling (aligned to those principles stated within section 3.8, 3.9 and 3.10).

3.13 Smart DCC's Information Classification and Handling Standard, which is mandatory reading for all Smart DCC staff, contractors and consultants, sets out the requirements for the identification, classification, management, storage and disclosure of Smart DCC's Confidential Information, and the management, storage and disclosure of 3rd party Confidential Information. The Standard additionally provides the controls which must be in place to protect the confidentiality, integrity and availability of information to ensure compliance with Smart DCC's legal, regulatory and contractual obligations.

3.14 Because of increased levels of remote working arising from the COVID-19 pandemic, additional mandatory training and guidance has been provided to all Smart DCC staff, contractors and consultants to ensure that the same standards of information security and handling are maintained when working remotely.

3.15 All contracts with Smart DCC agents, consultants, and contractors include obligations for the protection and management of Confidential Information. All such people who work on Smart DCC premises and with Smart DCC's information undertake the same training as DCC employees. DCC is mindful of its obligations to ensure its staff, contractors and its Service Providers are aware of and will act on their obligations.

4. Information Management Systems

4.1 The smart metering communications infrastructure provides the interface between Service Users and consumer smart meters. The infrastructure is presented to Service Users as a number of interfaces through which communications data may be sent. Message data sent by service users is validated and transformed before being sent to the smart meters. A similar process is followed for the return path.

4.2 All Confidential Information is processed under the principle of 'least privilege' whereby access is only granted to those users with an approved justification, i.e. where such access is necessary to fulfil their role. By default, logical and physical controls prevent access to information unless such access is explicitly granted.

4.3 All Smart DCC systems have been procured for the sole use of smart metering. The Smart DCC IT systems are separated from other systems used by other divisions of Capita plc or their customers. Logical access controls are in place to ensure that only authorised and authenticated users have access and that data remains segregated.

4.4 Communications and data systems are provided to the Smart DCC by external service providers who are governed by Smart DCC in terms of their compliance to applicable regulations, including the Smart Energy Code and the Smart Meter Communication Licence.

4.5 Smart DCC are responsible for ensuring that all information, assets, processes or information systems used for the purposes of carrying on the Authorised Business are certified to ISO/IEC 27001:2013. This includes DCC's production environment and all supporting test environments and systems. This is supported by the Smart DCC Information Security Management system (ISMS) which ensures ongoing compliance to all security obligations through internal audits, monitoring through internal Governance Risk and Compliance tools, practise reviews and working groups.

4.6 Privileged IT system administrators who support Smart DCC systems (which includes those employed by our external service providers) are tasked with maintaining the appropriate system security and segregation. All such privileged users have a greater level of access to system configuration and in some cases Smart DCC data and are therefore cleared to HM Government Security Clearance (SC) level. Alongside privileged users, all staff who are engaged in Security Operations, or whose roles require regular access to Smart DCC's most sensitive information and systems, are also cleared to SC level.

4.7 The Smart DCC office environments are separated from those of other Capita plc business units in order to maintain the principle of least privilege. Buildings access control systems are in place at all Smart DCC sites to ensure that no unauthorised individuals can gain access to the Smart DCC office environments.

4.8 Security related activity such as authentication and access events within smart metering information systems are recorded and monitored in Smart DCC's Security Operations Centre (SOC) in order to detect any weaknesses in the system that may result in breaches of confidentiality. This monitoring is part of the overall Smart DCC service management function and is carried out by Smart DCC teams who have received appropriate training to be able to detect and manage incidents appropriately. Incident Management is undertaken through Smart SCC's Incident Management process.

4.9 Any suspected breach of information systems or unauthorised disclosure is recorded as a security incident and investigated by the Smart DCC Security Operations Centre. If an investigation identifies any unauthorised disclosure or access to Confidential Information, appropriate remedial action is taken which includes notification or escalation to key stakeholders, including in compliance with data protection legislation where applicable. Remedial action of this kind may include the use of external forensic investigators when necessary, to identify issues, and the utilisation of DCC's Major Incident Management (MIM) framework, where a response is led by a multi-disciplinary team comprising Operational and Security staff under the direction of DCC's Executive Committee members.

4.10 All Confidential Information processed by Smart DCC is included within the scope of the Smart DCC Information Security Management System (ISMS) which is used as the framework for the management of all information systems. As required by the Smart Energy Code, the Smart DCC Information Security Management System shall be certified to ISO 27001:2013 by an independent UKAS accredited body and assured through internal and external review.