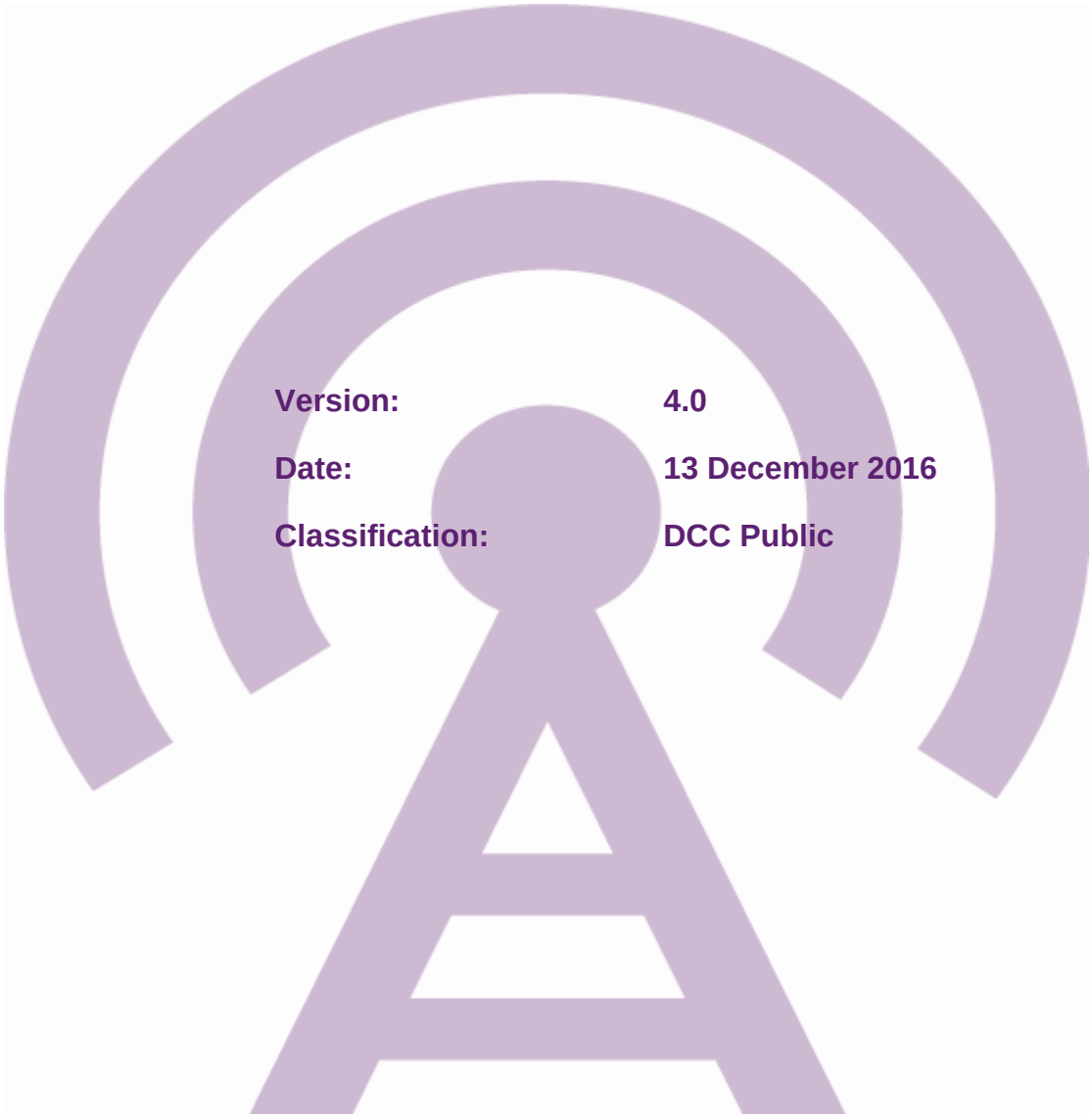
Data Communications Company

# Smart DCC Ltd

## Information Security Policy



| | |
|---|---|
| **Version:** | **4.0** |
| **Date:** | **13 December 2016** |
| **Classification:** | **DCC Public** |

# 1 Introduction

1.1 This Information Security Policy (ISP) defines the Smart DCC Ltd (Smart DCC) approach to information security. An effective ISP provides a sound basis for defining and regulating the protection of information.

1.2 Information security is defined as anything that affects the confidentiality, integrity, or availability of Smart DCC information assets and intellectual property:

- **Confidentiality** means ensuring information is only accessed by those authorised to do so;
- **Integrity** means safeguarding the accuracy and completeness of information;
- **Availability** means ensuring authorised individuals have access to information when required.

1.3 This ISP applies across all organisational elements in support of Smart DCC's Authorised Business (as defined by the Smart Meter Communications Licence), whether delivered internally or through a supplier. It applies to all staff, whether permanent or temporary, whilst engaged in support of the Smart DCC Authorised Business.

# 2 Information Security Policy Statement

2.1 Smart DCC acknowledges that information is a critical business asset and that protecting information assets, and satisfying applicable requirements relating to information security, are key reputational and operational priorities.

2.2 Smart DCC must therefore ensure that its working practices protect the organisation and its information assets from all threats whether internal, external, deliberate or accidental.

# 3 Information Security Objectives

3.1 Smart DCC implements and maintains an Information Security Strategy which provides the organisation with a roadmap for the protection of its information and IT systems. This strategy has helped to identify the following Smart DCC information security objectives for 2016-17 which have been set by the Chief Information Security Officer (CISO) and approved by the Board:

a. Maintain the Smart DCC Information Security risk management regime in accordance with ISO/IEC 27005:2011 to allow for the appropriate identification and management of risks associated with all Smart DCC information assets and IT systems

b. Maintain the Smart DCC Information Security Management System in a manner which allows for the continuous assessment of the effectiveness

of security controls and maintains its capability to be certified ISO/IEC 27001:2013.

c. Develop the operational security capability in a manner which supports the Smart DCC release strategy and continually improves to support new capabilities and mitigates evolving risks.

d. Establish and maintain the security relationship with the Smart Metering user community.

e. Provide appropriate support for all DCC Programme related activities in order to ensure that the organisation is equipped with the appropriate knowledge to make risk-based strategic security decisions.

f. Maintain Smart DCC senior management and Board level awareness of DCC IS obligations, risks and strategic initiatives.

g. Maintain a Smart DCC Information Security budget which continues to align to the DCC business needs and provides a cost-effective use of resources

# 4 Key Principles

4.1 The ISO/IEC 27001:2013 information security management standard shall be used as the basis for the Information Security Management System (ISMS).

4.2 Subsidiary information security policies, standards and procedures for specific activities and systems which support this Policy, shall be developed, communicated and implemented.

4.3 Risk assessments shall be conducted to identify and manage risks in accordance with the Smart DCC Information Security Risk Management Standard.

4.4 All information will be assessed for business impact and classified. It will be stored, processed, transferred and retained accordingly.

4.5 All providers of DCC services shall be governed appropriately with respect to their contractual security obligations.

4.6 All appropriate commercial, legislative, regulatory and contractual requirements shall be identified and met.

4.7 All staff, whether permanent, temporary or contract shall be educated in and made aware of, Information Security, their individual responsibilities and the need to remain compliant to subsidiary policies, standards and procedures.

4.8 The ISMS and its objectives shall be continually monitored to ensure that appropriate improvements are made.

# 5 Responsibilities

5.1 Smart DCC Board:

a. Owns this Policy and has ultimate accountability for its implementation as part of the Smart DCC Information Security Framework.

5.2 Smart DCC Managing Director:

a. Has overall responsibility for managing Smart DCC's activities and is responsible for its information security programme, including compliance with all relevant legislation.

5.3. Smart DCC Chief Information Security Officer (CISO):

a. Is responsible for aligning security initiatives with Smart DCC programmes and business objectives, ensuring that information assets and technologies are adequately protected.

b. Coordinates the development and maintenance of information security policies and standards.

c. Ensures Smart DCC is compliant with the security requirements of the Smart Meter Communication Licence and Smart Energy Code (SEC)

5.4. Smart DCC senior management team:

a. Have full responsibility for managing all activities under their control and deploying good practice approaches in accordance with this Policy.

b. Will engage suitable third parties to provide specialist services necessary to comply with the requirements of this Policy.

5.5. Smart DCC Information Security Team:

a. Ensures the Smart DCC ISMS remains appropriate, is operated effectively and conforms to the requirements of the ISO/IEC 27001:2013 standard, Capita plc Baseline Information Security Standards and information security good practice.

b. Ensures that appropriate systems for managing information security are developed, implemented, monitored and reviewed.

c. Facilitates ongoing improvement and compliance with legal, regulatory and other requirements to which the organisation subscribes.

d. Provides information security advice and support throughout Smart DCC.

5.6. All Smart DCC staff:

a. Are responsible for complying with the Smart DCC Information Security Policy, and subsidiary Smart DCC Policies, Standards and Procedures.

# 6 Policy Review and Communication

6.1. This Policy will be reviewed by the Policy owner on an at least annual basis. An intermediate review may be conducted at any time should it be deemed necessary by events either internal or external to Smart DCC.

6.2. Publication of a new version of this Policy will be controlled and communicated by the Smart DCC Information Security Team.

# 7 Compliance

7.1. If a deviation or exception is required to this Policy, then the prior written approval of the CISO must be obtained.

7.2. Failure to comply with this Policy or any supporting policy without such permission may result in disciplinary and/or criminal proceedings.

# 8 Document Control

| Revision Date | Summary of Changes | Author | Version No. |
|---|---|---|---|
| 17/11/2013 | Issued | Steve Johal | 1.0 |
| 19/02/2015 | Major update from version 1.0. | Steve Johal | 2.0 |
| 14/07/2015 | Major update following ISO27001 Stage 1 Audit | Steve Johal | 3.0 |
| 13/12/2016 | Update of objectives and minor changes | Peter Hammond | 4.0 |

# 9 Approvals

| Name | Title | Signature | Version No. |
|---|---|---|---|
| Jonathan Simcock | Smart DCC Managing Director |  | 4.0 |
| Marc Avery | Chief Information Security Officer |  | 4.0 |