Data Communications Company

Information Security Policy

Version: 5.1
Date: 04.08.20
Owner: Security GRC Team
Author: informationsecurity@smartdcc.co.uk
Classification: DCC Public

Think Secure, share Secure, respect Secure... live Secure.

Document Control

Revision history

Revision date	Summary of changes	Changes marked	Version number
01/10/2020	2020 revision.	No	5.0
27/7/2021	New DCC format. Added RACI, Related Docs section, expanded policy statement	Yes	5.1

Reviews

Name	Title / Responsibility	Release Date	Version number
Dax Costello	Security GRC Lead	06/08/2021	5.1
Dave Watkins-Hilton	Head of GRC	06/08/2021	5.1
Ian Speller	Director of Security	06/08/2021	5.1

Approvals

Name	Title / Responsibility	Release Date	Version number
Angus Flett	CEO	06/08/2021	5.1
Neil Dudleston	CISO	06/08/2021	5.1

Date of Next Review: August 2022

Our policies are independently audited as per our audit schedule. All new policies and amendments are approved by one of the following committees: ExCo, Board and ARC. The DCC Internal Audit and Controls Team can advise on the appropriate body.

Table of Contents

1. Introduction

1.1. Objective

The Information Security Policy defines Smart Data Communications Company Ltd.'s (DCC) approach to information security and establishes the basis upon which DCC manages and improves its information security capabilities.

1.2. Scope

All DCC information, assets, staff, contractors, business partners and Board members supporting DCC and DCC's authorised business activities (as defined by the Smart Energy Code (SEC)[1] and the Smart Meter Communication License[2] (Licence) conditions).

1.2.1. Out of Scope

Not applicable.

1.3. Communication

This policy will be reviewed as per guidelines from DCC Business Improvement and Internal Audit Team or a review may be conducted at any time should it be deemed necessary by events either internal or external to DCC.

The DCC Security Governance, Risk and Compliance (GRC) Team will own and review this policy.

DCC Security Team will be responsible for communicating this policy to relevant parties.

2. Policy

Any exceptions to this policy must follow the process in Section 2.3.

2.1. Policy Statement

This information security policy statement is to outline DCC Board's intentions to ensure DCC minimises cyber security risks and damage caused by security incidents.

DCC Board acknowledges its accountability in ensuring DCC information assets, services and supporting capabilities are:

- protected with proportionate risk-based confidentiality, integrity and availability controls
- appropriate threat intelligence, policies and controls communicated to interested parties
- security breaches are managed effectively
- applicable legislative, regulatory (including but not limited to SEC and License conditions) and contractual requirements are satisfied

[1] https://smartenergycodecompany.co.uk

[2] Smart Meter Communication Licence (ofgem.gov.uk)

- DCC aligns with proactive threat protection whether internal, external, deliberate or accidental and have adopted the NIST Cybersecurity Framework (CSF)[1] to provide a threat led approach:

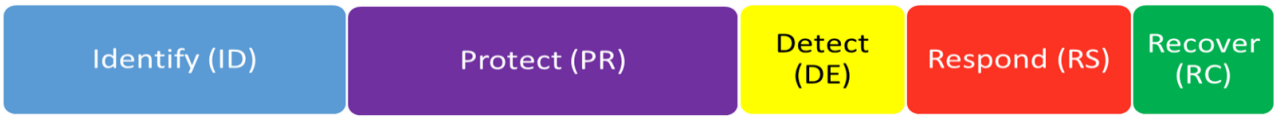

Figure 1 - NIST Cyber Security Framework

- The NIST CSF is mapped and aligned to ISO/IEC27001– Information technology — Security techniques — Information security management systems — Requirements (ISO27001) under which DCC is required to maintain certification as a License requirement.
- The DCC Security Framework maps all the relevant frameworks (NIST, ISO, SEC, etc.) that DCC uses or is required to use.
- The implementation of this policy is achieved through the Information Security Management System (ISMS) as defined within ISO27001 and which is described in the DCC ISMS Manual and Target Operating Model (TOM).
- The ISMS will be monitored via internal and external audit to ensure that it adheres to the objectives of this policy statement.

ID - Identify

Objective	**To ensure DCC information assets and supporting internal and external capabilities are identified and afforded proportionate and complaint risk-based protection through formal governance processes**

ID.AM Asset Management - The data, personnel, devices, systems, and facilities that enable the DCC to achieve business purposes are identified and managed consistent with their relative importance to organisational objectives and the DCC risk strategy.

ID.BE Business Environment – DCC's mission, objectives, stakeholders, and activities are understood and prioritised; this information is used to inform cybersecurity roles, responsibilities, controls and risk management decisions.

ID.GV Governance and Compliance - The policies, controls, processes and procedures to manage and monitor DCC's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

ID.RA Risk Assessment – DCC understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), DCC's assets, and individuals.

ID.RM Risk Management Strategy – DCC's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

[1] https://www.nist.gov/cyberframework

ID.SC Supply Chain Security – DCC's priorities, constraints, risk tolerances, and assumptions are established, and controls and processes implemented to identify, assess, manage and support risk decisions associated with managing supply chain security.

PR - Protect

Objective	**To incorporate continual improvement in security policies, controls and processes enabling resilience and Innovation in DCC Services and fostering a strong security culture influencing internal and external stakeholders (including their supply chain) to be ahead of prevailing threats.**

PR.AC Identity Management and Access Control - Access to physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access to authorised activities and transactions.

PR.AT Awareness and Training – DCC's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

PR.DS Data Security - Information and records (data) are managed with sharing restricted to authorised parties to avoid both malicious and unintended distribution, consistent with DCC's risk strategy, legislative and regulatory requirements and controls to protect the confidentiality, integrity, availability, ethical collection, aggregation, use, disclosure and destruction of data.

PR.IP Information Protection Controls, Processes and Procedures – Innovative and effective security controls, processes, and procedures are sponsored, maintained and used to manage protection of information systems and assets.

PR.MA Maintenance - Maintenance and repairs of information system components are performed consistent with policies, controls and procedures.

PR.PT Protective Technology - Technical security solutions are sponsored and managed to ensure the security and resilience of systems and assets are consistent with related legislative and regulatory requirements, policies, controls, procedures, and agreements.

DE - Detect

Objective	**To ensure logical and physical security is continuously assessed, monitored and tested to predict and promptly detect anomalies, threats and security risks**

DE.AE Anomalies and Events - Anomalous activity is predicted and promptly detected and the potential impact of events, threats and security risks is understood.

DE.CM Security Continuous Monitoring - Information systems and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

DE.DP Detection Processes - Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

RS - Respond

Objective	To ensure timely and effective containment and resolution of detected cyber security incidents

PS.RP Response Planning - Response controls, processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

PS.CO Communications - Response activities are appropriately communicated and coordinated with internal and external stakeholders (e.g. the SEC Panel and the Security Sub Committee).

RS.AN Analysis - Analysis is conducted to ensure effective response and support recovery activities.

RS.MI Mitigation - Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

RS.IM Improvements - DCC response activities are improved by incorporating lessons learned from current and previous detection/response activities.

RC - Recover

Objective	To ensure continual preparedness and improvement for recovery from cyber security incidence

RC.RP Recovery Planning - Recovery controls, processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

RC.IM Improvements - Recovery planning and processes are improved by incorporating lessons learned into future activities.

RC.CO Communications - Restoration activities are appropriately communicated and coordinated with internal and external parties (e.g. the SEC Panel and the Security Sub Committee, Internet Service Providers, owners of attacking systems, victims, supply chain and vendors).

2.2. Compliance

DCC CISO will be responsible for implementing this policy.

2.3. Exceptions

Exceptions to this policy must be authorised by the person responsible for approval of the policy.

Exceptions to this policy may be granted if:

a. Compliance would adversely affect the ability of the service to accomplish a mission critical function.
b. Compliance would have an adverse impact on the service provided or supported by the information, system, or resource.
c. Compliance cannot be achieved due to the incapability of the information system or resource.

All exception requests must be submitted to the Security GRC Team at their shared inbox informationsecurity@smartdcc.co.uk and quote the basis for the exception.

Where an exception is applicable, an information security risk assessment will be required, and the necessary approvals given by the business owner, system owner and the Security Team. Evidence of the risk assessment and approval must be archived and available for audit purposes.

Where Material Changes have been made to this policy, 6 months from approval of the change is granted to achieve compliance. Material Changes are listed in Appendix A – Material Changes and defined in Section 4 -Definitions.

3. RACI

Responsible	Accountable
• *CISO* • *Security GRC Team*	• *CEO*

Consulted	Informed
• *Security Team* • *Third Parties*	• *All DCC staff (permanent/ contractor /contingent worker)* • *Public information (published on www.smartdcc.co.uk)*

Note that a comprehensive Information Security Management System (ISMS) RACI has been drawn up for the DCC ISMS in its entirety.

4. Definitions

Acronym	Definition
ARC	Audit and Risk Committee
CEO	Chief Executive Officer
CISO	Chief Information Security Officer
CSF	Cyber Security Framework
DCC	Smart DCC Ltd.
ExCo	Executive Committee
GRC	Governance, Risk and Compliance
ISMS	Information Security Management System
ISO27001	ISO/IEC27001– Information technology — Security techniques — Information security management systems — Requirements
License	Smart Metering Communication License
Material Change	A change in the meaning or language of the controls within this standard that may result in incurrence of development, implementation and management costs
NIST	National institute of Standards and Technology, U.S. Department of Commerce
SEC	The Smart Energy Code
TOM	Target Operating Model

5. Related Documents

- The Smart Energy Code
- Smart Metering Communication License
- ISO/IEC27001– Information technology — Security techniques — Information security management systems — Requirements
- DCC Security Framework
- Information Security Management System (ISMS) RACI
- DCC ISMS Manual
- DCC Target Operating Model

Appendix A - Material Change

Change No	Original Ref	Original Content	New Ref	New Content	Comments