Data Communications Company

Information Security Policy

SECURITY FUNCTION – POL049

1. Introduction

1.1. Policy Purpose

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.

2. Policy Statement

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

3. 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], Retail Energy Code (REC)[2] and the Smart Meter Communication Licence[3] (Licence) conditions).

3.1. Out of Scope

Not applicable.

4. RACI

Responsible	Accountable	Consulted	Informed
Security Function	CISO	Other DCC Functions, relevant stakeholders	All staff, contractors, and consultants. Public

5. Principles

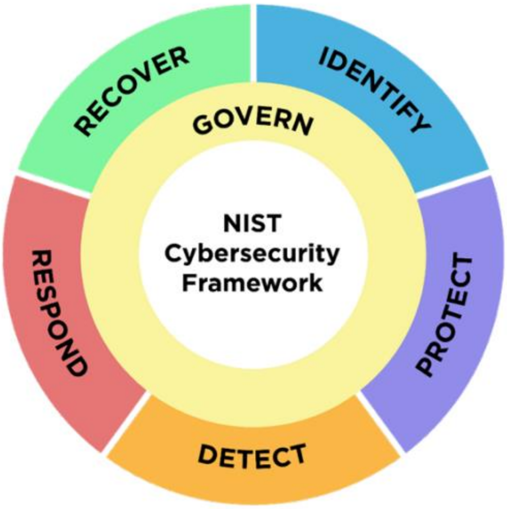
The DCC Board acknowledges its accountability in ensuring DCC information assets, services and supporting capabilities are:

- Protected with proportionate risk-based confidentiality, integrity, and availability controls.
- Managed through appropriate threat intelligence, policies and controls communicated to interested parties.
- Managed effectively with regards to security breaches.
- Compliant with applicable legislative, regulatory (including but not limited to SEC, REC, and Licence conditions) and contractual requirements.
  Aligned with proactive threat protection whether internal, external, deliberate, or accidental and have developed the DCC Security Architecture Framework (aligned with several

[1] https://smartenergycodecompany.co.uk
[2] REC Portal
[3] Smart Meter Communication Licence (ofgem.gov.uk)

frameworks including the NIST Cybersecurity Framework (CSF) 2.0 to provide a threat led approach.

Figure 1 – NIST Cybersecurity Framework (CSF) 2.0



- The NIST CSF 2.0 is mapped and aligned to ISO/IEC27001:2022 – Information Security, CyberSecurity & Privacy Protection — Information Security Management Systems — Requirements (ISO27001) under which DCC is required to maintain certification as a Licence requirement.
- The DCC Security Architecture 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 DCC Operating Model (OM).
- The ISMS is to be monitored via internal and external audit to ensure that it adheres to the objectives of this policy statement.

5.1. GV – Govern

Objective	The organisation’s cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored
GV.OC	Organisational Context - The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organisation’s cybersecurity risk management decisions are understood
GV.RM	Risk Management Strategy - the organisation’s priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions
GV.RR	Roles, Responsibilities, and Authorities - Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated

GV.PO	Policy - Organisational cybersecurity policy is established, communicated, and enforced
GV.OV	Oversight - Results of organisation-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy
GV.SC	Cybersecurity Supply Chain Risk Management - Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organisational stakeholders

5.2. ID - Identify

Objective	The organisation's current cybersecurity risks are understood
ID.AM	Asset Management – Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to organisational objectives and the organisation's risk strategy
ID.RA	Risk Assessment – The cybersecurity risk to the organisation, assets, and individuals is understood by the organisation
ID.IM	Improvement - Improvements to organisational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions

5.3 PR - Protect

Objective	Safeguards to manage the organisation's cybersecurity risks are used
PR.AA	Identity Management, Authentication, and Access Control - Access to physical and logical assets is limited to authorised users, services and hardware and managed commensurate with the assessed risk of unauthorised access.
PR.AT	Awareness and Training – The organisation's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks
PR.DS	Data Security – Data are managed consistent with the organisation's risk strategy to protect the confidentiality, integrity, and availability of information
PR.PS	The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organisation's risk strategy to protect their confidentiality, integrity, and availability
PR.IR	Security architectures are managed with the organisation's risk strategy to protect asset confidentiality, integrity, and availability, and organisational resilience

5.4 DE - Detect

Objective	Possible cybersecurity attacks and compromises are found and analysed
DE.CM	Continuous Monitoring –Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.
DE.AE	Adverse Event Analysis – Anomalies, indicators of compromise, and other potentially adverse events are analysed to characterise the events and detect cybersecurity incidents

5.5 RS - Respond

Objective	Actions regarding a detected cybersecurity incident are taken
RS.MA	Incident Management - Responses to detected cybersecurity incidents are managed
RS.AN	Analysis – Investigations are conducted to ensure effective response and support forensics and recovery activities
RS.CO	Response activities are coordinated with internal and external stakeholders (e.g., the SEC Panel and the Security Sub Committee) as required by laws, regulations, or policies
RS.MI	Incident Mitigation – Activities are performed to prevent expansion of an event, and mitigate its effects

5.6 RC - Recover

Objective	Assets and operations affected by a cybersecurity incident are restored
RC.RP	Incident Recovery Plan Execution – Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents
RC.CO	Incident Recovery Communication – Restoration activities are 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).

6. Exceptions

Exceptions to this policy must be authorised by the DCC's CISO.

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 may be 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.

All exceptions must be documented including approvals and signoffs from relevant stakeholders.

7. Compliance Monitoring

The DCC's CISO is responsible for implementing this policy and maintaining compliance through processes operated by the Security Function.

8. Communication

The Policy is communicated to all stakeholders by being published on Policy Hub and on the DCC's external website.

9. Definitions

Term	Description
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/IEC27001:2022– Information, Security, CyberSecurity & Privacy Protection— Information Security Management Systems — Requirements
Licence	Smart Metering Communication Licence
NIST	National institute of Standards and Technology, U.S. Department of Commerce
REC	Retail Energy Code
SEC	The Smart Energy Code
OM	Operating Model

Related Documents

- The Smart Energy Code
- The Retail Energy Code
- Smart Metering Communication Licence
- ISO/IEC27001:2022 — Information, Security, CyberSecurity & Privacy Protection — Information Security Management Systems — Requirements
- DCC Security Architecture Framework
- Information Security Management System (ISMS) RACI
- DCC ISMS Manual
- DCC Operating Model