Data Communications Company

Information Security Policy Statement

October 2019

Version:	**5.0**
Owner:	**Smart DCC CISO**
Approved by	**Smart DCC CEO**
Classification:	**DCC Public**
Next Review	**October 2020**

1 Introduction

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

1.1 Scope

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

1.2 Exceptions

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

Exceptions to this Policy must be obtained in writing from the Chief Information Security Officer (CISO).

[1] https://smartenergycodecompany.co.uk/
[2] Smart Meter Communication Licence

2 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 communicate to interested parties
- security breaches are managed effectively
- applicable legislative, regulatory (including but not limited to Smart Energy Code (SEC)[3] and License[4] conditions) and contractual requirements are satisfied

DCC aligns with proactive threat protection whether internal, external, deliberate or accidental and have adopted the NIST Cybersecurity Framework (CSF)[5] to provide a threat led approach:

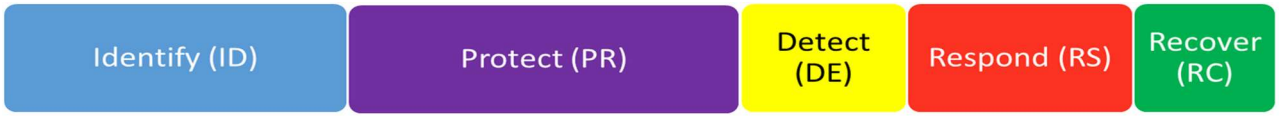

Figure 1 - NIST Cyber Security Framework

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.

[3] https://smartenergycodecompany.co.uk/
[4] Smart Meter Communication Licence
[5] https://www.nist.gov/cyberframework

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

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).