1. Introduction

Purpose

Smart DCC Ltd (DCC) protects its information, systems and services through a risk-based information security programme aligned to ISO 27001 and NIST Cyber Security Framework (CSF). Everyone working for or on behalf of DCC must support and comply with this policy.

2. Policy

The DCC Board is committed to protecting DCC's information and reducing the risk and impact of security incidents.

3. Scope

This policy applies to:

- All DCC information and information systems
- All DCC employees
- Contractors, consultants and business partners working for DCC
- Board members
- Activities carried out under DCC's regulatory obligations

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

What this means for staff

Everyone who works for or on behalf of DCC must:

- Follow DCC security policies and procedures.
- Protect information from unauthorised access.
- Report suspected security incidents immediately.
- Complete mandatory security awareness training.
- Use DCC systems responsibly.

5. Principles

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

- Protected by security controls that match the level of risk.
- 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[1], REC[2], and Licence[3]) and contractual requirements
- Protected against threats from inside and outside the organisation, whether intentional or accidental.

5.1. Framework

DCC manages information security using the DCC Security Architecture Framework (SAF) which is aligned with NIST CSF 2.0[4] and ISO/IEC 27001[5]. The framework supports six core activities.

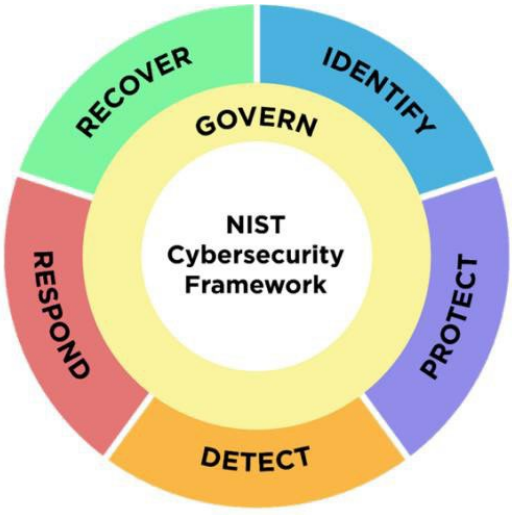

Figure 1 – NIST Cybersecurity Framework (CSF) v2.0

- The SAF maps all the framework and applicable legislative and regulatory requirements 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 ISMS Manual and Security Operating Model (SOM).
- The ISMS is monitored via internal and external audit to ensure that it adheres to the policy statement.

[1] SEC The Smart Energy Code - Smart Energy Code
[2] REC Home - The Retail Energy Code Company
[3] Licence Smart Meter Communication Licence | Ofgem
[4] NIST CSF 2.0 Cybersecurity Framework | NIST
[5] ISO/IEC 27001 ISO/IEC 27001:2022 - Information security management systems

6. Exceptions

The CISO must approve any exception to this 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 Governance, Risk and Compliance (GRC) Team at 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 Function. 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. The GRC Team, reporting to the CISO, manages day-to-day compliance activities.

8. Communication

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

9. Continual Improvement

DCC continually improves its Information Security Management System by reviewing risks, objectives and controls to ensure they remain effective and meet business and regulatory requirements.

10. Policy Responsible Person

For any queries related to this policy, please contact the designated policy author listed in the DCC Policy Hub, who is best placed to provide clarification or additional guidance or contact informationsecurity@smartdcc.co.uk.

11. Definitions

Term	Description
ARC	Audit and Risk Committee
CEO	Chief Executive Officer
CISO	Chief Information Security Officer
CSF	Cybersecurity Framework
DCC	Smart DCC Ltd. (Data Communications Company)
ExCo	Executive Committee
GRC	Governance, Risk and Compliance
ISMS	Information Security Management System
ISO27001	ISO/IEC27001:2022– Information, Security, Cyber Security & 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	The Retail Energy Code
SEC	The Smart Energy Code
SOM	Security Operating Model

12. Related Documents

- The Smart Energy Code
- The Retail Energy Code
- Smart Metering Communication Licence
- ISO/IEC27001:2022 —Information Security Management Systems
- DCC Security Architecture Framework
- National Institute of Standards and Technology CSF v2.0
- Information Security Management System (ISMS) RACI
- ISMS Manual
- Security Operating Model