Information Security Policy

Smart DCC Ltd acknowledges that information is a critical business asset, and that protecting our information assets is a key reputational and operational priority. We must ensure, that at all times, our working practices protect Smart DCC Ltd and its information assets from all threats whether internal, external, deliberate or accidental.

Information Security is defined as:

Anything that affects the Confidentiality, Integrity, and Availability, of Smart DCC Ltd's information assets and intellectual property:

- *Confidentiality means ensuring data is only accessed by those authorised to do so.*
- *Integrity means safeguarding the accuracy and completeness of information.*
- *Availability means ensuring authorised workers have access to information and systems when require.*

Information Security means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction. The terms Information Security, Computer Security and Information Assurance are frequently used interchangeably.

Information Security does not only cover Information Technology (IT) systems. It also consists of the following areas:

- Physical Security, which includes perimeter controls, building security (including clear desk policies) and access to secure zones.
- Procedural Security covering topics such as operating procedures and acceptable use policies.
- Personnel Security, which includes training, vetting, security clearance (where required), aftercare, escorting and the potential for disciplinary actions and / or criminal proceedings.
- Technical Security covering topics such as IT based identification, authentification, access control, penetration / vulnerability testing and monitoring.

Smart DCC Ltd appropriately and effectively secure our information assets, and those we are responsible for, through adoption, implementation and enforcement of applicable law and relevant and commonly acknowledged Information Security best practices.

We shall review, measure and monitor our Information Security framework, documentation and implemented controls, on an annual basis, to assure their continual relevance and effectiveness in protecting our information assets.

Information Security Policies and Standards will provide the framework to ensure the protection of Smart DCC Ltd information assets. This policy will be underpinned by a series of Security

Standards which provide the detailed requirements for implementation (for which ISO27001:2005 certification will be sought):

Technical security

- Antivirus
- Application Development & Security
- Audit Logging and Monitoring
- Authentification
- Backup Management
- Database Security
- Encryption
- Firewall Management
- IT Equipment Disposal
- IT Equipment Transport and Delivery
- Mobile Device Security
- Network and Telecoms
- Password
- Patch Management
- Removable Media
- Security Testing
- Server and Endpoint Security
- Website Security
- Wireless

Data management security

- Asset Classification and Handling
- Business Continuity Planning
- Confidential Information Disposal
- Data Retention
- Incident Response
- Third Party Management

Physical security

- Access Passes and Identity Cards
- Barriers
- Car Park
- CCTV
- Control of Access
- Mail Handling and Post Room
- Physical Intruder Detection System
- Secure Areas
- Security Lighting

Jonathan Simcock
Managing Director