Information Security Policy

The purpose of this information security policy (the "Policy") is to give strategic direction and to define commitment to the safe operational delivery of CSSC products and services. This commitment is given to employees, to our customers and partners and key interested parties.

The objective of the Information Security Management System (ISMS) is to ensure the confidentiality, integrity, and availability of information assets[1], through the implementation of controls and procedures, which support this Policy.[2] The Policy is therefore critical to our business success, and that of our clients.

It is the goal of CSSC Sports & Leisure to ensure that:

- Information assets are protected and controlled against unauthorised access or misuse.
- Confidentiality of information assets is assured.[3]
- Integrity and availability of information assets is maintained.[4]
- Planning processes are maintained to secure information assets in the event of a Business Continuity invocation.
- Regulatory, contractual, and legal requirements are complied with.[5]
- Role dependant Information Security training is provided to all employees.
- All appropriate resources needed for the ISMS are provided.
- The ISMS is embedded into the business and is part of business as usual.
- Physical, logical, environmental and communications security is maintained.[6]
- Operational procedures and responsibilities are regularly maintained and improved.
- All information security incidents (breaches, threats, weaknesses, or malfunctions) are reported to the Leadership Team (LT) and investigated through appropriate processes.
- Infringement of this Policy may result in immediate disciplinary action or criminal prosecution.
- Business requirements for the availability of information and information systems are met.
- The ISMS effectiveness is regularly reviewed by leadership and improved as appropriate

The Chief Executive Officer has approved and supports this Policy and has overall responsibility for its implementation. The Group Financial Controller has direct responsibility for maintaining this Policy and providing guidance and advice on its implementation. Senior Managers are responsible for the implementation of this Policy within their business area. Trusted sources are used to provide direction on the contents of the system's policies and procedures, and these will include but are not limited to certification standards, professional bodies, service requirements and service providers and partners.

It is the responsibility of each employee to adhere to this Policy.

Endorsed by Alastair Smart
Group Financial Controller
Date: May 2021

NOTES:
1. Information assets are stored physically and electronically, transmitted across networks or telephone lines, sent by fax, spoken in conversations, and printed as hardcopy.
2. These will be outlined and maintained within the ISMS and regularly reviewed (at least annually).
3. Valuable and sensitive information will be protected against unauthorised access and disclosure.
4. Safeguards will be created to protect against unauthorised modification and destruction of information.
5. This ensures compliance with the legal requirements of the Copyright, Design & Patents Act 1988, Data Protection Act 1998, the Computer Misuse Act 1990, the Companies Act 1989 and any other relevant legislation (see business legal register).
6. Controls exist to prevent unauthorised access, damage, and interference of IT services.