

Information Security Policy Statement

(One-page excerpt taken from Appendix B of the
SG Fleet Group Information Security Policy V4.0)

SG Fleet Group Limited
ABN 40 167 554 574

18 September 2023

SG Fleet Group Limited (SG Fleet) conforms to the ISO 27001:2013 and ISO 27001:2022 standard, which is reflected in its Information Security Policy. As part of the standard, SG Fleet has implemented an Information Security Management System (ISMS), which is a formal system to protect the confidentiality, integrity and availability of information.

SG Fleet is committed to continually maintaining and maturing its ISMS to comply with applicable legal and other obligations to which it subscribes, and to satisfy the expectations of interested parties as outlined in its ISMS Framework.

SG Fleet's Management is committed to providing continuous support to achieve its ISMS objectives and strives to develop and implement relevant and viable information security policies, procedures and controls, ensuring that:

- Information security risks are managed proactively by conducting regular risk assessments and implementing cost-effective controls to mitigate unacceptable risks identified.
- The availability of information and information systems is met, as required by its core and supporting business operations.
- The confidentiality of information is assured.
- The integrity of information is maintained.
- Appropriate access control is maintained, and information is protected against unauthorised access.
- All exploits and vulnerabilities are remediated as soon as possible.
- Acceptable legal and contractual requirements are met.
- Information security education, awareness, and training is available to SG Fleet staff and a requirement of their employment.
- Information security incidents are promptly handled through an efficient incident management process.
- All breaches of information security, actual or suspected, will be reported to and investigated by the relevant internal teams and authorities where mandated.
- Information security continuity is part of the Business Continuity Plan to counteract interruptions to business activities and to protect critical business processes from the effects of major information failures or disasters.
- Continuous proactive information security improvements are conducted with regular internal audits and management reviews.

This Policy Statement is available to all staff and to any interested parties, as part of SG Fleet's commitment to its information security.

The Information Security and Cyber Risk Committee (ISCR) is responsible for reviewing and updating this Policy Statement in line with SG Fleet's Information Security Policy and supporting documentation.

Paul dos Santos
Chief Information Security Officer

Kevin Wundram
Chief Financial Officer and Head of Risk