Information Security Policy Statement v1

CG-P-44

This policy applies to all companies under Churchill Contract Services Group Holdings Ltd to include the following subsidiaries and trading names:

- Churchill Contract Services (CCS)
- Amulet (Churchill Security Solutions) (AMU)
- Churchill Environmental Services (CES)
- Churchill Contract Catering t/a Radish (RAD)
- Chequers Contract Services Ltd (CHE)
- Chequers Electrical & Building Services Ltd (CEBS)

Churchill Group is committed to satisfying, and wherever possible, exceeding client expectations and to ensuring that the services offered meet their specific contractual requirements, together with the relevant requirements of ISO 27001:2013 and any other applicable statutory and regulatory requirements, including the UK General Data Protection Regulation (UK GDPR) and current Data Protection Act (2018).

It is the policy of the Company to provide services of a quality that will merit and earn client satisfaction, enabling the Company to both retain its existing clients and to generate new clients, via a policy continual improvement of within the Information Security Management System (ISMS) policies, procedures and working practices.

All Company personnel share a responsibility for the security of the services provided to its clients, and reasonable access will be provided to client representatives to review the Company's working practices in relation to specific contractual requirements.

Information is vital to the way in which the Company conducts its business. As the custodian of client and employee information that is potentially sensitive, the Company has a fundamental responsibility to protect and manage this information from unauthorised modification, loss, or accidental or deliberate disclosure in compliance with the requirements of the UK GDPR and the Data Protection Act 2018 and to enable the Company to meet its contractual, legislative, privacy and ethical responsibilities.

It is essential that reliable and accurate information is made available for Company staff to conduct their day-to-day business. To achieve this requirement the Company has introduced an ISMS with the aim of protecting both the Company's reputation, and the efficiency and effectiveness of its business operations, and the confidentiality, Integrity and availability of all client and Company information.

All Company assets – hardware, software, documents, personal information – are subject to a detailed risk assessment on an on-going basis, and all new assets will be subject to a risk assessment and added to the Information Asset Risk Assessment Register.

The Churchill Board owns the ISMS. The Information Security Management Team (ISMT) is responsible for monitoring its day-to-day operation, for its on-going review and improvement, and is the main point of contact for the reporting of all security problems and incidents. The Board is represented on the ISMT by the Chief Operating Officer.

The ISMT in partnership with the Quality Team is also responsible for the administration of the ISMS documentation, and for management of outsourced ISMS services covering internal audits, liaison with the external certification body and management review activities.

The ISMT is responsible for the approval of the information security objectives and measures their achievement via a series of associated metrics and performance data. This Team is also responsible for the identification and assessment of information security risks and their relative priorities, for responding to them promptly and for implementing appropriate and effective security safeguards and controls in a timely manner.

The HR Director, via the recruitment and induction processes, is responsible for ensuring that all employees are fully aware of the importance of information security in relation to business activities and for the provision of information security-related training.

All staff and visitors are required to comply with ISMS policies and procedures as appropriate to them – the level of compliance achieved is monitored on on-going basis by the ISMT – and for reporting any weaknesses or areas for improvement to the ISMT for consideration.

Churchill Group will ensure that its activities can continue with minimal disruption, or other adverse impact, should it suffer any form of disruption or security incident.

This policy will be formally reviewed annually and updated as required.

Signed on behalf of Churchill Contract Services Group Holdings Ltd

J.M. Briggs, Group Managing Director

Date: July 2022