Information Security Policy

Introduction

Chandlers Information Security Policy applies to all business functions within the scope of the Information Security Management System and covers the information, information systems, networks, physical environment and people supporting these business functions. This document states the Information Security objectives and summarises the main points of the Information Security Policy.

Objective

The objective of Information Security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. In particular, information assets must be protected in order to ensure:

- Confidentiality i.e. protection against unauthorised disclosure
- Integrity i.e. protection against unauthorised or accidental modification
- Availability as and when required in pursuance of the Organisation's business objectives.

Responsibilities

The Managing Director has approved the Information Security Policy.

Overall responsibility for Information Security rests with the Information Security Manager.

Day-to-day responsibility for procedural matters, legal compliance including data protection, maintenance and updating of documentation, promotion of security awareness, liaison with external organisations, incident investigation, management reporting etc. rests with the Information Security Manager.

Day-to-day responsibility for technical matters, including technical documentation, systems monitoring, technical incident investigation and liaison with technical contacts at external organisations, rests with the Information Security Manager in conjunction with a specialised third party computer organisation.

All employees or agents acting on the Organisation's behalf have a duty to safeguard assets, including locations, hardware, software, systems or information, in their care and to report any suspected breach in security without delay, direct to the Information Security Manager. Employees attending any location that is not occupied or owned by the Organisation must ensure the security of the Organisation's data and access their systems by taking particular care of PDAs, laptops and/or similar computers they have in their possession, together with any information on paper or other media.

The Information Security Manager is responsible for drafting, maintaining and implementing this Security Policy and similarly related policy documents as detailed in Appendix II.

As with other considerations including Quality and Health & Safety, Information Security aspects are taken into account in all daily activities, processes, plans, contracts and partnerships entered into by the Organisation.

The Organisation's employees are advised and trained on general and specific aspects of Information Security, according to the requirements of their function within the Organisation. The Contract of Employment includes a condition covering confidentiality regarding the Organisation's business.

The Information Security procedures as set out in the Organisation's Information Security Manual and the Staff Handbook detail the contractual duty of all employees. The employee signs their Contract of Employment to acknowledge acceptance of all rules, policies and procedures relating to employment within the Organisation.

Copies of this Manual, including the Risk Assessment (Annex A Appendix) are made available to all of the Organisation's employees.

Breach of the Information Security policies and procedures by the Organisation's employees may result in disciplinary action, including dismissal.

In view of the Organisation's position as a trusted supplier of enforcement agent services, particular care is taken in all procedures and by all employees to safeguard the Information Security of its service users and/or clients.

Agreements of Mutual Non-disclosure/Confidentiality are entered into, as appropriate, with third party companies.

All statutory and regulatory requirements are met and regularly monitored for changes.

Information Security Policy

A Disaster Recovery/Business Continuity Plan is in place. This is maintained, tested and subjected to regular review by the Information Security Manager.

Further policies and procedures such as those for access, acceptable use of e-mail and the internet, virus protection, backups, passwords, systems monitoring, etc. are in place, maintained and are regularly reviewed by the Information Security Manager or an appointed representative, as appropriate.

This Information Security Policy is regularly reviewed and may be amended by the Managing Director in order to ensure its continuing viability, applicability and legal compliance, and with a view to achieving continual improvement in the Information Security Systems.

Signed:  Dated: 6th January 2016

Mr C Waterman CICM, MIoD
Managing Director
Chandlers Limited