ISO 27001 INFORMATION SECURITY POLICY

Introduction

The Organisation's 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:

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

Responsibilities

1. The Chief Executive Officer has approved the Information Security Policy.
2. Overall responsibility for Information Security rests with the CEO.
3. Day-to-day responsibility for procedural matters, legal compliance, maintenance and updating of documentation, promotion of security awareness, liaison with external organisations, incident investigation and management reporting etc. rests with the ISMS Manager (Head of Operations).
4. Day-to-day responsibility for data protection rests with the Data Protection Officer.
5. 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 Internal IT Manager).
6. 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 ISMS Manager (Head of Operations). Employees attending sites that are not occupied by the Organisation must ensure the security of the Organisation's data and access their systems by taking particular care of laptop and similar computers and of any information on paper or other media that they have in their possession.
7. The ISMS Manager (Head of Operations) is responsible for drafting, maintaining and implementing this Security Policy and similarly related documents.
8. As with other considerations including Quality and Health & Safety, Information Security aspects are taken into account in all daily activities, processes, plans, projects, contracts and partnerships entered into by the Organisation.
9. 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.

10. Adherence to Information Security procedures as set out in the Organisation's various policies and guideline documents is the contractual duty of all employees and a clause to this effect is set out in the Organisation's Contracts of Employment.

11. Copies of this Management System, including the Risk Assessment (Statement of Applicability) are made available to all of the Organisation's employees.

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

13. In view of the Organisation's position as a trusted provider of digital transformation, user adoption and IT services, particular care is taken in all procedures and by all employees to safeguard the Information Security of its service users and/or clients.

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

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

16. A Disaster Recovery/Business Continuity Plan is in place. This is maintained, tested and subjected to regular review by the ISMS Manager (Head of Operations).

17. 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 ISMS Manager (Head of Operations) or an appointed representative, as appropriate.

18. This Information Security Policy is regularly reviewed and may be amended by the ISMS Manager (Head of Operations) or CEO in order to ensure its continuing viability, applicability and legal compliance, and with a view to achieving continual improvement in the Information Security Systems.

Policy Sign-off

Date of Issue:	27/10/2020
Date of Next Review:	30/09/2021
Name:	Tim Barber
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	30/09/2020	Jo Holloway	
2.0	27/10/2020	Jo Holloway	Updated responsibilities and date