sprint Logistics

Information Security Policy

Sprintlogistics.com

The Sprint Logistics Information Security Policy applies to all business functions within the scope of the information Security Management System and covers the information, information systems and 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.

Aizad Hussain - CEO

Objective

The objective of Information Security is to ensure the 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 organisations business objectives.

Certification

Sprint is certified under the data Protection Act 1998.

Registration Number – ZA166659

Responsibilities

1. The Managing Director has approved the Information Security Policy

2. Overall responsibility for Information Security rests with the IT manager

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

4. All employees or agents acting on the organisations 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 Quality Manager. Employees attending any location that is not occupied or owned by the organisation's data and access their systems by taking particular care of any electronic devices issued to them, together with any information on paper or other media.

5. The Quality Manager is responsible for drafting maintaining and implementing the security policy and similar related policy documents.

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

7. The organizations 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 organisations business.

8. The Information security procedures as set out in the organisations information security manual details the contractual duty of all employees. The employee's sign their Contract of employment to acknowledge acceptance of all rules, policies and procedures relating to employment within the organisation.

9. Copies of this policy are made available to all employees via the intranet.

10. Breach of the Information Security policies and procedures by the Organisations employees may result in disciplinary action, including dismissal.

11. In view of the organisations position as a trusted supplier for the provision of storage and distribution, fulfilment and international mail, worldwide courier services, call centre services and design and print, particular care is taken in all procedures and by all employees to safeguard the Information Security of its service users and or clients.

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

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

14. A disaster recovery/business continuity plan is in place. This is maintained, tested and subjected to regular review by the IT manager and quality manager.

15. Further policies and procedures such as those for access, acceptable use of e-mail and the internet, virus protection, back-ups, passwords, systems monitoring, etc are in place, maintained and are regularly reviewed by the IT manager or an appointed representative.

16. This information security policy is regularly reviewed and may be amended by the managing director or his nominated representative, in order to ensure its continuing viability, applicability and legal compliance, and with a view to achieving continual improvement in the Information Security Systems.