ISO 27001:2005
INFORMATION SECURITY MANAGEMENT POLICY STATEMENT

St John Cymru - Wales

Introduction

The **St John Cymru - Wales Patient Transport Services** Information Security Management Policy applies to all business functions within the scope of the System and covers the people, physical infrastructure, virtual infrastructure and information supporting these business functions. This document states the Information Security Management objectives and summarises the main points of the Information Security Management Policy.

Policy statement

We are committed to maintaining and continually improving an Information Security Management System (ISMS) that satisfies applicable requirements and is certified to the international standard ISO 27001:2005.

We will conduct our operations in accordance with the demands of our ISMS and will comply with all legislation, reasonable practice, client policies, standards and statutory and other obligations where required and relevant to our activities and the jurisdictions in which we operate.

Purpose

This policy aims to prevent and minimise the impact of security incidents and business disruptions in order to ensure we provide a service that meets or exceeds the expectations of our customers. We manage and control our information security risks to protect and preserve the confidentiality, integrity and availability of information.

Responsibilities

1. The Chief Executive is responsible for ensuring the implementation of this policy.

2. The Senior Management Team is responsible for taking measures to help staff act in compliance with this policy. Line managers are required to check that their staff are aware of this policy.
3. All staff are required to comply with the policy requirements and share responsibility for our performance in implementing it.
4. The Senior Management Team, all staff members, clients, contractors and third parties are expected to take responsibility for the security of organisational information.

Implementation

We maintain our ISMS within an Integrated Management System (IMS) that also controls and documents our quality, environmental and health and safety management processes. Our IMS is a documented system with defined processes and procedures designed to control and review our activities. All IMS policies, procedures and documents are accessible by all staff via the on-line management system.

1. We operate a risk assessment process that is documented and controlled.
2. The organisation establishes ISMS objectives and reviews performance against them.
3. We provide adequate resources to establish, implement, maintain and improve the ISMS.
4. We conduct internal audits of our ISMS in accordance with our planned audit schedule.
5. We assess the continuing suitability, adequacy and effectiveness of our ISMS via regular management reviews.

St John
Cymru - Wales

Responsibilities

1. The Chief Executive has approved the Information Security Management Policy.
2. Overall responsibility for monitoring the Information Security Management System including procedural matters, legal compliance, maintenance and updating of documentation, promotion of awareness, liaison with external organisations and incident investigation rests with the Quality Manager Designate.
3. As with other considerations including those relating to Quality, the Environment, Health & Safety and Business Continuity aspects are taken into account in all daily activities, processes, plans, projects, contracts and partnerships entered into by the Organisation.
4. The Organisation's employees are advised and trained on general and specific aspects of Information Security Management, according to the requirements of their function within the Organisation. The Contract of Employment includes a condition covering confidentiality regarding the Organisation's business.
5. Adherence to Information Security Management procedures as set out in the Organisation's various policies and documents is considered to be a contractual duty of all employees.
6. Copies of this Manual are made available to all of the Organisation's employees.
7. Breach of the Information Security Management policies and procedures by the Organisation's employees may result in disciplinary action, including dismissal.
8. In view of the Organisation's position as a trusted provider of complete patient transport services provider, particular care is taken in all procedures and by all employees to ensure that Information Security Management remains integral to all business activities.
9. All statutory and regulatory requirements are met and regularly monitored for changes.

Signed by ..... **Date**.....18 May 2017.....

pp

Keith Dunn OBE (Chief Executive)