# Information Security Policy

## 1. Introduction

This information security policy shall apply to information, systems, networks, applications, locations and staff of Horizon Strategic Partners.

The purpose of this policy is to enable and maintain effective security and confidentiality of information processed or stored by Horizon Strategic Partners. This shall be achieved by:

- Ensuring that all members of Horizon Strategic Partners staff are aware of and shall comply with relevant legislation, including the Data Protection Act (2018).
- Describing the principles of information security management and describing how they shall be implemented within Horizon Strategic Partners.
- Assisting staff to identify and implement information security as an integral part of their day to day role within Horizon Strategic Partners.
- Safeguarding information relating to staff and patients that Horizon Strategic Partners are able to access.
- Complying with all Data Controller responsibilities as required by The Data Protection Act 2018 and associated contracts.

## 2. Objectives

Key objectives of this Information Security Policy are to preserve:

- **Confidentiality** - Access to information shall be restricted to those staff of Horizon Strategic Partners and relevant others with agreed authority to view it.
- **Integrity** – Records are to be complete and accurate with all filing and management systems operating correctly.
- **Availability** - Information shall be readily available and delivered to the authorised recipient, when it is needed.

## 3. Responsibilities for Information Security

- Responsibility for information security shall rest with the Horizon Strategic Partners Directors. However, on a day-to-day basis the IG Lead shall be responsible for organising, implementing and managing this policy and its related good working practices.
- The IG Lead shall be responsible for ensuring that both permanent and temporary staff including any contractors and locums are aware of:-
    - The information security policies applicable to their work areas

- Their personal responsibilities for information security
- Who to ask or approach for further advice on information security matters.

- All staff shall abide by security procedures of Horizon Strategic Partners. This shall include ensuring that confidentiality and integrity are not breached. Failure to do so may result in disciplinary action.
- This Information Security Policy document shall be owned, maintained, reviewed and updated by IG Lead. This review shall take place annually. The results of which shall be made known to the Horizon Strategic Partners Directors with overall responsibility for security.
- Staff of Horizon Strategic Partners shall be responsible for both the security of their immediate working environments and for security of information systems they use [eg workstations, laptops, PDAs, cardex etc].
- Any contracts with third party organisations that allow access to the information systems of Horizon Strategic Partners, shall be in place before access is allowed. These contracts shall ensure that the staff or sub-contractors of those external organisations shall comply with all the appropriate security policies / guidance required by Horizon Strategic Partners.

**Horizon Strategic Partners shall undertake to ensure:**

1. **Contracts of Employment –** address information security requirements at the recruitment stage and that all contracts of employment shall contain a confidentiality clause. The information security requirements shall be included within job descriptions.

2. **Access Controls -** to areas containing information systems are restricted and controlled to ensure that only those authorised can access confidential information.

3. **Equipment Security –** is effective in order to minimise losses, or damage to the Horizon Strategic Partners. All information assets and equipment shall, where possible be physically protected from security threats and environmental hazards. (Locked cabinets (fire proof if possible), clear desk policy and the limitation of risks in the surrounding work area etc).

4. **Information Risk Assessment –** a regular assessment of the working environment shall be conducted to identify potential risks to the security of Horizon Strategic Partners information. Where risks are identified, these should be noted and where possible mitigating action taken.

5. **Security Incidents and weaknesses -** are to be recorded and reported to the IG Lead so that they can be investigated to establish their cause, impact and the effect on Horizon Strategic Partners and accessible systems. (NB. remedial changes arising may need to be

included within future staff working procedures, updates to policies and contracts of employment).

6. **Protection from Malicious Software –** should be provided through the use of commercial strength anti-virus/anti-malware software. Where there is an internet connection an appropriate firewall shall be installed and managed. No new software shall be downloaded or installed on computer systems of Horizon Strategic Partners without the explicit permission of IG Lead. Breach of this requirement may be subject to disciplinary action.

7. **Secure Communications –** should be in place to ensure that all correspondence, faxes, email, telephone messages and transfer of confidential records are conducted in a secure and confidential manner. All communication of NHS Confidential or NHS restricted information by email must be appropriately protected, using cryptographic controls (AES 256 bit or equivalent).

8. **Business Continuity and Disaster Recovery Plans –** are in place so that in the event of a disruption to the information services of Horizon Strategic Partners, it is possible to activate relevant business contingency plans until affected services are restored.

9. **Unauthorised Use of NHS Confidential or NHS Restricted data contained in any Horizon Strategic Partners developed applications** – by any Horizon Strategic Partners staff is prohibited. Breach of this requirement may be subject to disciplinary action.

**Policy approved by:**

Signature

Eamus Halpin, Director, Horizon Strategic Partners

Date

Horizon Strategic Partners