Healthcare Gateway Information Security Policy

Information security overview

Healthcare Gateway is committed to establishing, implementing, operating, monitoring, reviewing and maintaining an Information Security Management Systems (ISMS). The scope of certification for ISO27001 includes the main Healthcare Gateway Office at Fulford Grange and Grianan House, Dundee Technology Park, Gemini Crescent, Dundee.

The Healthcare Gateway business includes:

- Provision and development of clinical information and management systems to healthcare professionals;
- Support services to Healthcare Gateway customers
- Providing managed services
- Providing Project / Implementation management services.

The information security management activities for Healthcare Gateway will include management of the following premises: HS3 Stable Block, Fulford Grange, Rawdon and Dundee Technology Park, Gemini Crescent, Dundee.

The information we gather in the course of these activities is our most valuable asset. Our reliance upon information means we must ensure that we keep it confidential, so as to maintain its security, integrity and accessibility at all times. This Information Security Policy Statement sets the ground rules required to meet these obligations within a well-defined Information Security Management System.

Information security aims

It is Healthcare Gateway's policy to develop, implement and maintain an Information Security Management System that is aligned to Healthcare Gateway's measurable objectives:

- Provides assurance within the company and to our customers and suppliers that the confidentiality, integrity and availability of their information will be maintained appropriately.
- Manages information security risks to all company and customer assets by basing information security decisions and investments on risk assessment of relevant assets considering; confidentiality, integrity and availability.
- Applies appropriate control to maintain the security of information security assets.
- Takes into account business and legal or regulatory requirements and contractual security obligations.
- Protects the company's ongoing ability to meet contracted commitments through appropriate business continuity planning.

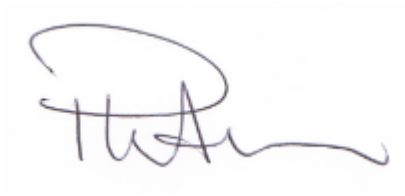
- Maintains awareness of all employees so they can identify and fulfil contractual, legislative and company specific security management responsibilities.
- Deals effectively with security incidents to minimise the business impact.
- Ensures commitment to continual improvement.

This policy is supported by the following:

- A company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001:2013 Standard for Information Security Management Systems.
- An Information Security Risk Assessment Process that assesses the business harm likely to result from a security failure and the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and controls currently implemented.
- Setting and regular review of achievement of information security objectives
- Defined security controlled perimeters and access to controlled offices and facilities to prevent unauthorised access, damage and interference to business premises and information.
- Data classification and exchange guidance within the Information Security Procedure including compliance with regulations under the Data Protection Act 1998 to protect client, partner, supplier, our own and personal employee information which is not in the public domain.
- Development and maintenance of an appropriate Business Continuity Plan to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.
- Information security awareness guidance for all company employees.
- Implementation of incident management and escalation procedures for reporting and investigation of security incidents for ISMS management review and action.
- A senior management team that supports the continuous review and improvement of the company ISMS.

This Information Security Policy is communicated to all person(s) working for or on behalf of Healthcare Gateway (as part of induction training) and is available to all employees in the IMS folder.

It is reviewed as or when there are key changes (e.g. in customer, legislative, operational requirements etc) and annually as a minimum by the senior management team who recommend amendments and updates to the policy as part of the Review and continuous service improvement process.



Signed:

Managing Director

Date: 10th January 2017

Disclaimer

Contact information

Healthcare Gateway, Fulford Grange, Micklefield Lane, Rawdon, Leeds, LS19 6BA.
enquiries@healthcaregateway.co.uk
www.healthcaregateway.co.uk
0845 601 2642