Aquila Heywood

Information Security Management System Policy

24 July 2017

Table of Contents

1 Background

As an organisation, we:

- Collect, process, store, and transmit information.
- Recognise that information, and related processes, systems, networks and people are important assets for achieving organisation objectives.
- Have a legal duty to protect certain types of information.

In our connected world, information held and processed is subject to threats of attack from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, error, nature (for example, flood or fire) and so on, and is subject to vulnerabilities inherent in its use.

Damage to information systems and networks caused by malicious code, computer hacking and denial-of-service attacks have become more common, more ambitious and increasingly sophisticated.

The term 'Information Security' is generally based on information being considered as an asset, which therefore has a value and requires appropriate protection. In reviewing Information Security, three main properties are considered:

- Confidentiality: Information is not made available or disclosed to unauthorised individuals, entities, or processes.
- Integrity: Protecting the accuracy and completeness of information assets.
- Availability: Information is accessible and usable upon demand by an authorised entity.

Achieving Information Security requires the management of risk and encompasses risks from physical, human and technology-related threats associated with all forms of information within or used by the organisation.

Our business, technology, and information are all dynamic in nature and subject to changing risks over time. Learning from an ongoing review of Information Security (for example, any security incidents, results of risk management or known vulnerabilities) helps to make our Information Security Management System (ISMS) more effective.

The coordinated activities directing the implementation of suitable controls and managing Information Security risks are generally known as elements of our ISMS.

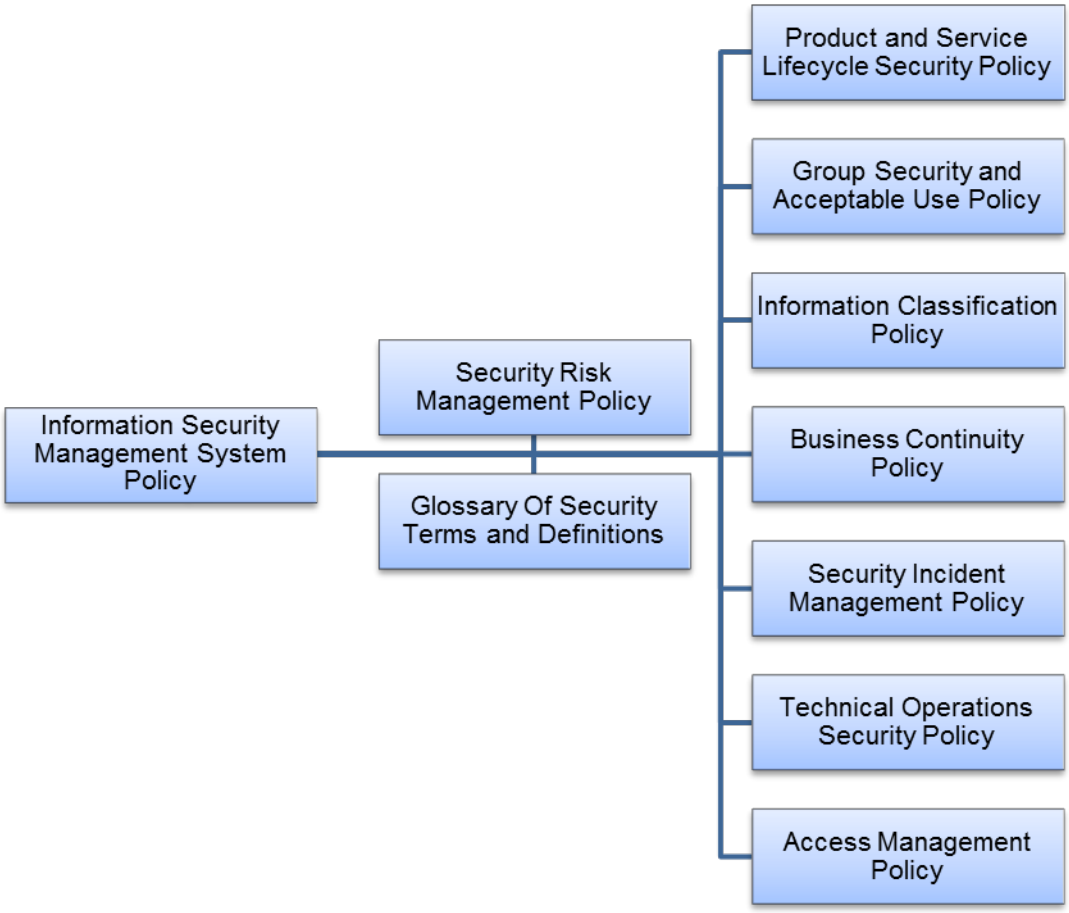
2 Information Security Management System (ISMS)

The Aquila Heywood Information Security Management System (ISMS) is the term used to describe all the policies, procedures, resources and other parts of the organisation that implement, maintain, review and improve Information Security.

The ISMS is integrated with the Quality Management System (QMS) and they are jointly referred to as the Aquila Heywood management system.

This Information Security Management System Policy and other ISMS policies are organised in a framework to separate them according to their scope and the people to whom they are relevant.

Graphical illustration of the ISMS structure



The requirements in these security policies are based on risks to Aquila Heywood information assets and good security practice. Controls to mitigate these risks are monitored by the manager responsible for the system, process or other type of control to ensure they remain effective.

All staff are responsible for adhering to the ISMS Policy; managers must ensure their area of responsibility is compliant with the ISMS.

The ISMS shall be reviewed in line with internal audit procedures and appropriate improvements implemented.

Information Security risks shall be managed in the context of Aquila Heywood's overall business risk.

Documentation of the ISMS will be managed in line with the QMS.

2.1 Objectives and measures

The Information Security Management System has the following objectives and measures:

Objective	Measure
Assure the confidentiality of customer information in the care of Aquila Heywood.	Information Security requirements identified, specified, built and tested within all service implementations. Information security incidents recorded within the Group Incident Management system and reported to stakeholders – Security and Quality Forum and customers, if appropriate.
Protect the confidentiality of Aquila Heywood information.	
Protect the integrity of information held by Aquila Heywood.	
Maintain availability of information to stakeholders according to requirements.	
Ensure legal and regulatory security requirements are identified and met.	Review of appropriate requirements with the Group Legal Counsel
Enable the planning and testing for continuity of services to customers and internal business services in the case of a major incident or disaster.	Successful annual testing of the recovery of services to the DR/Test data centre. Evidenced by customers.
Provide effective Information Security training, education and awareness.	New staff introduced to the ISMS with confirmed annual statement of review. Staff with specific security roles appropriately trained and skilled.
Identify potential and actual breaches of Information Security, investigate and take appropriate action to report, remedy and/or prevent similar incidents.	All security incidents recorded in the Group Incident Management system.
Inform senior management of the effectiveness of the ISMS.	Circulation of Security and Quality Forum minutes to the Executive Management Committee
Work continuously to improve in everything we do	Internal audit programme

3 Scope

The sales and marketing, customer management, supply, implementation, development, enhancement, support, hosting and customer operational management of the Life and Pensions systems products and services provided by Aquila Heywood, including the provision of Data Screening and Cleansing services and data validation through the ATMOS organisation and data management services via i-Connect.

The management of security covers all areas within the technical and physical boundaries as stated in the Information Security Management System Policy.

3.1 Technical boundaries

The Redhill and Altrincham office services and infrastructure, including internal and external hosted services, wireless networks, remote access services, inter-site links and customer connections.

The use of Aquila Heywood remote services and mobile devices by staff of the Group.

The architecture and design of products created by the Aquila Heywood Group.

3.2 Physical boundaries

The Redhill and Altrincham offices, including the machine rooms at those sites, together with the transfer of any sensitive data in our care outside the office perimeters.

4 ISMS roles, responsibilities and authority

The **Group's Security Consultant** is responsible for the day-to-day management of the ISMS, its regular review and continuous improvement.

The Security Consultant shall work with Heads of Department to implement and maintain the ISMS such that effective and efficient controls are in use, and report status as required to senior management.

Department Heads are responsible for the processes and/or technical controls that protect the security of information and assets in their area.

They will ensure that the ISMS policies are applied in their area and inform the Security Consultant of any incidents that affect the ISMS's effectiveness, and propose any changes necessary for its continual improvement.

In particular, managers shall:

- Classify the information for which they are responsible.
- Define appropriate access rights to that information.
- Manage the risks to their information and assets as agreed with the Security Forum.

The **Security and Quality Forum** is the group responsible for providing leadership on, reviewing the operation of, and approving any changes to the ISMS. The Security and Quality Forum comprises the Security Consultant, Quality Manager, CTO and Director | People and is chaired by the CFO.

The Security and Quality Forum governs the ISMS within Aquila Heywood.

The Security and Quality Forum is accountable for:

- Setting direction and priorities on security matters
- Authorising changes to security policy and procedures
- Reviewing the security awareness program
- Management of security incidents
- Monitoring the programme for registration to ISO27001
- Reviewing Information Security risk assessments and improvement plans

- Maintaining the Group Security Risk Register
- Considering improvement actions to enhance the ISMS
- Monitoring the management of vulnerabilities
- Receiving and reviewing Information Security-related audit reports

The quorum of the Security and Quality Forum is three members; a quorate Security and Quality Forum has authority regarding security management.

The Security and Quality Forum shall review the management of risks and the effectiveness of controls to mitigate these at least quarterly.

The security policies are reviewed annually, or when required, to ensure they remain relevant and effective. Changes to the security policies are authorised by the Security and Quality Forum.

Any member of staff may suggest improvements to the ISMS via their line manager or a member of the Security and Quality Forum.

Aquila Heywood, Aquila House, 35 London road, REDHILL RH1 1NJ
W: www.aquilaheywood.co.uk T: 01737 859859

Aquila Heywood