Information Security Management System (ISMS)

PHX034

1. Contents

2. Document Control

2.1 Purpose of the System

The purpose of the Information Security Management System (ISMS) is to provide an overview of Phoenix's approach to information security management in compliance with ISO 27001:2013 requirements. This is a key information document describing how the scope of the management system is defined, providing a framework for the management of security policies, security objectives, roles and responsibilities and information security procedures. It acts as a reference guide for employees and stakeholders, providing guidance on how we protect our sensitive information and manage information security risks.

2.2 Scope

The system applies to all employees, contractors, suppliers, third-party service providers, and any other parties with access to the organisation's information.

3. Context of the Organisation

3.1 Understanding the organisation and its context

Established in 1990, Phoenix Software Ltd provides IT solutions to markets including Public Sector, Voluntary and Charities, Housing, Education and Corporate sectors.

In December 2020 Phoenix became part of the Bytes Technology Group PLC, with over 350 employees working out of the Yorkshire based office, remotely or to a hybrid pattern.

The IT Solutions offered to our customers include the resell of industry standard software licensing and hardware, consultancy (Professional) and managed IT services across leading edge technologies including software asset management tooling and services.

Phoenix has considered the factors and issues that can affect the Information Security Management System, these comprise of the following:

Political Factors
Change of Government political parties and policies affect the spending patterns and decision making within Central and Local Government Authorities along with the NHS and other government bodies. These decisions may affect the timing and budgets of these organisations which may in turn influence the performance of Phoenix.

Economic Factors
The economic climate can influence the timing of purchasing new IT solutions or may reduce the budgets available for investment. Our sales and marketing strategies must allow us to adapt and adjust to reflect these changes by offering alternative cost-effective solutions.

Social Factors
Phoenix is one of the largest employers in the local area and our ethos is to employ locally where practicable and to support local businesses. The prevailing culture at Phoenix plays a crucial role in information security and Phoenix recognises that positive security culture encourages employees to prioritize security and be proactive in safeguarding information assets.

Technology Factors
The rate of technology change demands that Phoenix must continually upskill and ensure the latest technological solutions are offered to our customers. We must maintain our current supplier/vendor accreditations to remain a forerunner in the industry and monitor emerging technology offerings from new sources. Phoenix also has a software development team, developing applications for internal and external use, these applications must be designed and developed securely, made fit for purpose, and maintained.

Environmental Factors
Environmental factors are often beyond the direct control of Phoenix but still have a significant influence on our security posture. The cyber threat landscape can affect our risk profile and risk management strategies and security practices of vendors and suppliers can impact our overall security posture. Climate change and natural disasters can impact business operations and security measures.

Legislative and Contractual Factors
Phoenix is affected by government policies and legislation that determine the purchasing processes that are imparted onto our government authority customers. GDPR poses strict requirements on the privacy and data protection of staff and customers, and contractual agreements that include security provisions.

3.2 Understanding the needs and expectations of Interested Parties

Phoenix has determined:

a) interested parties relevant to the ISMS
b) the requirements of those interested parties relevant to information security

Interested parties are persons or organisations that can influence the information security of Phoenix or can be affected by our information security activities;

- **Employees and dependents** - Employee and next of kin data needs to be protected from compromise. Employees require a secure working environment and information security knowledge through guidance and nurturing, training, and sharing of contractual information to protect the confidentially, integrity and availability of the organisation's information and that of its customers.
- **Executive Committee/Board of Directors** - Investment in our people, processes, and technology to retain our security accreditations and develop and deliver secure solutions to our customers, in alignment with business objectives. To be fully committed to the success of the ISMS.

- **Neighbours** – Blenheim House is situated on a shared industrial estate. Neighbours may be concerned about the potential impact of security incidents or data breaches at Phoenix. Such incidents could lead to unintended consequences that affect local businesses such as disruption to services. Understanding boundaries and working collaboratively on security matters can enhance the physical security controls across the estate.
- **Shareholders and investors** – Trust in the security of the organisation to protect its financial performance and reputation.
- **Government agencies/regulators** - Compliance with applicable laws in relation to the organisation, such as the Information Commission Office; if personal data is compromised through a security breach, it must be reported to the ICO in a timely manner
- **Customers** – Customers need to protect their own data, therefore place trust in Phoenix to have a robust ISMS. They require Phoenix to remain in compliance with security policies and contractual security clauses.
- **Media** – The media requires timely, succinct, and transparent responses to major security incidents to negate opportunities for competitors to take advantage of. The appointed spokespeople of Phoenix must be accessible by the media to receive statements and press releases.
- **Suppliers** and sub-contractors - Phoenix and suppliers need equal assurance that sharing of information or handling of customer data is compliant with policy and regulation and does not compromise the security of its own or its customer's security and reputation.
- **Competitors** – Some of our competitors are geographically located within a 20-mile radius and they will seek advantage over us. Transfer of employees between organisations is restricted by contract of employment clauses, however, transfer of data is a risk. Phoenix must guard its security practices and maintain robust security controls to protect against this
- **Auditors and certifying bodies** - External auditors and certifying bodies will assess the effectiveness of our ISMS for compliance with certain security standards.
- **Insurers** – Our insurers need to understand our security posture when underwriting our cyber insurance.

3.3 Determining the scope of the Information Security Management System

The organisation has determined the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organisation considered:

a) the external and internal issues referred to in 4.1 of the Standard and 3.1 of this document
b) the requirements referred to in 4.2 of the Standard and 3.2 of this document
c) two-way confidence and compliance with information security between Phoenix and external organisations

The scope statement is available as a separate document.

The scope of the ISMS for Phoenix is as follows:

The Information Security Management System (ISMS) applies to all our services which include software licensing, managed services, hardware, Software Asset Management, and IT Consultancy.

The sectors serviced are Public Sector, Charities & Housing Associations and Education. Sales and services are delivered by the employees, systems and business processes within Blenheim House, York Road, Pocklington, York YO42 1NS

3.4 Information Security Management System

Our ISMS is sponsored, approved, and led by senior management and leadership team, and in accordance with ISO27001.

As part of the management system, regular reviews are undertaken to ensure the effectiveness and identification of improvements as required by the Standard, as well as changes to the business and interested parties.

4. Leadership

4.1 Leadership and commitment

Management of Phoenix demonstrate leadership and commitment with respect to the information security management system by:

- ensuring the information security policy and objectives are established and are in line with the strategic aims of the company
- ensuring the integration of the ISMS requirements into Phoenix processes
- ensuring that the resources needed are available
- communicating and conforming to the importance of an effective ISMS
- ensuring that the system achieves its intended outcomes
- directing and supporting all employees to contribute to the effectiveness of the system
- promoting continual improvement
- supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility

4.2 Policy

The Management of Phoenix has established an information security policy that:

- is appropriate to the purpose of the company
- includes information security objectives and provides the framework for setting the objectives
- includes a commitment to satisfy the requirements related to the Standard
- includes an assurance of continual improvement of the ISMS

The information security policy is:

- available as documented information on SharePoint
- communicated within the company
- available to interested parties, as deemed appropriate by the Information Security Committee

4.3 Organisation roles, responsibilities, and authorities

The Management of Phoenix ensures that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Management assign the responsibility and authority for:

- ensuring that the ISMS conforms to the requirements of the Standard
- reporting on the performance of the system to management

Information Security roles, responsibilities and authorities have been clearly identified and communicated to members of staff.

These are documented in the Information Security Manual.

5. Planning

5.1 Actions to address risks and opportunities

5.1.1 General

When planning for the ISMS, the company considers the issues referred to in 4.1 and the requirements referred to in 4.2 and determines the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcomes
b) prevent or reduce security incidents
c) achieve continual improvement

The company plans actions to address risks and opportunities utilising the ISMS processes. This includes measurement and evaluation for effectiveness.

The Information Security Committee meet at planned intervals to assess and evaluate the system, typically every six months.

The Information Security Management process for Risk Management and Risk Assessments is documented in the Information Security Risk Assessment and Methodology Policy located on SharePoint.

5.1.2 Information security risk assessment

Phoenix defines and applies an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:

1. the risk acceptance criteria
2. criteria for performing information security risk assessments

b) ensures that repeated information security risk assessments produce consistent, valid, and comparable results

c) identifies the information security risks:
   1. apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity, and availability for information within the scope of the system
   2. identify the risk owners

d) analyses the information security risks
   1. assess the potential consequences that would result if the risks identified in clause c) above were to materialise
   2. assess the realistic likelihood of the occurrence of the risks identified in clause c) above
   3. determine the levels of risk

e) evaluates the information security risks
   1. compare the results of risk analysis with the risk criteria established in clause a) above
   2. prioritises the risks for risk treatment

5.1.3 Information security risk treatment

Phoenix has defined and applied an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results
b) determines the mitigating actions that are necessary to implement the information security risk treatment option(s) chosen
c) compare the mitigating actions determined in clause b) above with those in Annex A and verify that no necessary controls have been omitted
d) produce a Statement of Applicability that contains the necessary controls (see clauses b) and c) above and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A
e) formulate an information security risk treatment plan
f) obtain the risk owners' approval of the information security risk treatment plan and acceptance of the residual risks

5.2 Information Security Objectives and planning to achieve them

Based on the evaluation of risks, vulnerabilities and opportunities for improvement, Phoenix has created several specific and measurable security objectives.

The information security objectives shall:

a) be aligned to business goals and consistent with the ISMS

b) take into account information security requirements and results from risk assessment and risk treatment
c) be communicated
d) be updated as appropriate

The company shall retain documented information on the information security objectives.

When planning how to achieve its information security objectives, the company shall determine:

a) what it is to be done
b) what resources are required
c) who is responsible
d) when it will be completed
e) how the results are evaluated

Objectives for Information Security are documented in the Information Security Policy located on SharePoint.

6. Support

6.1 Resources

Phoenix has allocated the resources required for the establishment, implementation, maintenance, and continual improvement of the ISMS.

Additional resource needs are covered as part of the Information Security Management Review.

6.2 Competence

The company has:

a) determined the necessary competence of person(s) doing work under its control that affects its information security performance
b) ensure that these persons are competent on the basis of appropriate education, training, or experience
c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken
d) retained appropriate documented information as evidence of competence

6.3 Awareness

Persons doing work under the company's control are aware of:

a) the information security policy

b) their contribution to the effectiveness of the ISMS, including the benefits of improved information security performance
c) the implications of not conforming with the ISMS requirements

All Staff at Phoenix are constantly made aware of Information Security and records of platform training are kept by Training Dept.

6.4 Communication

Phoenix has determined the following communications are required as part of the ISMS:

Internal Communications
- updates to ISMS
- updates from the Information Security Committee
- training

External Communications
- responses to customer enquiries
- information relating to security incidents to interested parties

6.5 Documented Information

6.5.1 General

The ISMS includes the documented information required by the ISO27001 standard as determined by Phoenix as being necessary for the effectiveness of the system.

6.5.2 Creating and Updating

The Information Security Committee is responsible for all documentation used in the system.

All documents must be approved by the Managing Director and the manager responsible for the area covered by the applicable document.

All documents must include the following document controls:

- title
- revision date
- revision number
- reference

Where possible all documents are electronic using standard company applications.

6.5.3 Control of documented information

Phoenix ensures the documentation required is controlled to ensure the relevant information is available and suitable for use and is adequately protected from loss of confidentiality, improper use, or loss of integrity.

The documented information is accessible for all members of staff however only authorised personal can make amendments.

7. Operation

7.1 Operational planning and control

The company has planned, implemented, and controlled the processes needed to meet information security requirements and to implement the actions determined in 5.1.

The company has also implemented plans to achieve information security objectives determined in 5.2.

The company keeps documented information, including risk assessment, planning and statement of applicability to have confidence that the processes have been carried out as planned.
The company has planned control changes and reviews the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The company has ensured that outsourced processes are determined and controlled.

7.2 Information Security Risk Assessment

The company performs information security risk assessments at planned intervals or when significant changes are proposed or occur.

The organisation retains documented information of the results of the information security risk assessments.

Information security risk assessments are performed by the Information Security Committee on an annual basis and as required due to changes in the company, systems, or processes.

This is documented in the Information Security Risk Assessment and Methodology Policy.

7.3 Information Security Risk Treatment

The company shall implement the Information Security Risk Treatment Plan.

The company shall retain documented information, where practicable, of the results of the information security risk treatment.

This is documented in the Information Security Risk Assessment and Methodology Policy.

8. Performance Evaluation

8.1 Monitoring, measurement, analysis, and evaluation

Phoenix evaluates the information security performance and the effectiveness of the ISMS.

The company determines:

a) what needs to be monitored and measured, including information security processes and controls
b) the methods for monitoring, measurement, analysis, and evaluation of the risk, as applicable, to ensure valid results NB: the methods selected should produce comparable and reproducible results to be considered valid.
c) when the monitoring and measuring shall be performed
d) who shall monitor and measure
e) when the results from monitoring and measurement are analysed and evaluated
f) who shall analyse and evaluate these results

The organisation retains appropriate documented information as evidence of the monitoring and measurement results.

8.2 Internal Audit

Phoenix conducts internal audits at planned intervals to provide information on whether the ISMS:

a) conforms to
    1. the company's own requirements for its ISMS
    2. the requirements of the Standard
b) is effectively implemented and maintained

Phoenix :

c) plans, establishes, implements, and maintains an audit programme, including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme takes into consideration the importance of the processes concerned and the results of previous audits
d) defines the audit criteria and scope for each audit
e) selects auditors and conducts audits that ensure objectivity and the impartiality of the audit process
f) ensures that the results of the audits are reported to the relevant management
g) retains documented information as evidence of the audit programme and the audit results

This is documented in the Internal Audit Policy.

8.3 Management Review

The Management reviews the company's ISMS annually to ensure its continuing suitability, adequacy, and effectiveness.

This forms the basis of the Information Security Management Review and includes consideration of:

a) the status of actions from previous management reviews
b) changes in external and internal issues that are relevant to the ISMS
c) feedback on the information security performance, including trends in:
    1. nonconformities and corrective actions
    2. monitoring and measurement results
    3. audit results
    4. fulfilment of information security objectives
    5. feedback from interested parties
d) results of risk assessment and status of risk treatment plan
e) opportunities for continual improvement
f) results and recommendations for security incidents

The outputs of the management review shall include decisions related to continual improvement opportunities and any need for changes to the ISMS.

The company retains documented information as evidence of the results of management reviews.

The agenda and documentation are put together by the Information Security Committee prior to the review.

Results from the Information Security Management Review are stored on SharePoint.

9. Improvement

9.1 Non-conformity and corrective action

When a non-conformity occurs, Phoenix carries out the following:

a) react to the non-conformity and as applicable:
    1. take action to control and correct it
    2. deal with the consequences
b) evaluate the need for action to eliminate the causes of non-conformity, in order that it does not reoccur or occur elsewhere, by:
    1. reviewing the non-conformity
    2. determining the causes of the non-conformity
    3. determining if similar non-conformities exist or could potentially occur
c) implement any action needed

d) review the effectiveness of any corrective action taken
e) make changes to the ISMS, if necessary

Corrective actions shall be appropriate to the effects of the non-conformities encountered.

Phoenix retains documented information as evidence of:

f) the nature of the non-conformities and any subsequent actions taken
g) the results of any corrective action

Non-conformities and corrective actions can be identified from any source including, IT, staff, users, customers, and suppliers.

Such non-conformities may be identified from (not exhaustive):

- technical reviews
- team meetings
- supplier meetings
- risk assessments
- Internal and external audits

Non-conformities and corrective actions are recorded in the Non-Conformity and Corrective Action log.

9.2 Continual Improvement

The company continually improves the suitability, adequacy, and effectiveness of the ISMS. This is based on the following PDCA methodology:

- The context of the organization, leadership, planning, and support - plan phase
- operations - do phase
- performance evaluation - check phase
- improvement - act phase

Continual Improvement is reviewed as part of the Information Security Management Review.

Version Control

Author	Version	Date	Description
ISC	1.0	01/07/2015	Original
ISC	2.0	25/09/2018	Annual review
ISC	3.0	01/04/2020	Annual review
ISC	3.0	14/09/2021	Annual review
ISC	3.0	09/08/2022	Annual review
Geoff McGann	4.0	18/07/2023	Renamed the document, reviewed Interested Parties

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	01/07/2015	Managing Director
Sam Mudd	2.0	25/09/2018	Managing Director
Sam Mudd	3.0	01/04/2020	Managing Director
Sam Mudd	3.0	14/09/2021	Managing Director
Clare Metcalfe	3.0	30/09/2022	Operations Director
Clare Metcalfe	4.0	24/07/2023	Operations Director

Signed:  Clare Metcalfe, Operations Director

Dated: 24/07/2023