Information Security Policy

PHX025

Contents

Information Security Management Policy........ 2
Purpose........ 2
Intended Audience........ 3
Scope........ 3
Definition........ 3
Objectives........ 4
Policy Compliance........ 5
Policy Governance........ 6
Version Control........ 7
Document Approval........ 7

Information Security Management Policy

Phoenix operates an Information Security Management System that ensures the confidentiality, integrity and availability of the information that is integral to the success of our business. The Information Security Policy encapsulates the processes and responsibilities associated to meeting ISO27001:2013.

Phoenix Software believes that all employees have a role working within the guidelines of ISO27001:2013 to protect and safeguard the information that is utilised and held within the confines of the business.

The ISMS is based on three fundamental requirements:

- **Confidentiality** – all business and personal information is deemed confidential and must be treated as such. Information must not be disclosed to third parties unless it is necessary for business purposes
- **Integrity** – business information must be kept updated and stored correctly
- **Availability** – procedures and access rights must be determined, and information made available to approved parties

To ensure that the policy is successfully implemented, risks regarding the systems, personnel And processes that affect our business information are assessed and managed accordingly.

Objectives needed to ensure that the requirements of the policy are met and that continued improvement is sought will be set, determined, and monitored by the senior management team through the Management Review process.

The Information Security Policy principles and objectives are communicated and made available to staff at all times. Training will be an integral part of the strategy to achieve the objectives.

We shall ensure that all our personnel understand and fully implement our Company policies and objectives and are able to perform their duties effectively through an ongoing training and development programme.

Purpose

Information is a major asset that Phoenix has a responsibility and requirement to protect.

Protecting information assets is not limited to covering the information (electronic data or paper records) that the company maintains. It also relates to the people that use them, the processes they follow, and the physical IT equipment used to access them.

This Information Security Policy addresses these areas to ensure that high levels of confidentiality, integrity and availability are maintained.

The policy details the basic requirements and responsibilities for the proper management of information assets at Phoenix. The policy also specifies the means of information handling and transfer by the company.

Intended Audience

This document is intended for all employees and interested parties in the Information Security Management System of Phoenix.

Scope

This Information Security Policy applies to all the systems, people and business processes that make up the company's information systems. This includes all employees, contractual third parties and agents of the company who have access to information systems or information used for Phoenix purposes.

Definition

This policy is applied whenever information systems or information are utilised. Information can take many forms that include, but is not limited to, the following

- hard copy data printed or written on paper
- data stored electronically
- communications sent by post / courier or using electronic means
- stored tape or video
- conversation

Objectives

Phoenix recognises that there are risks associated with users accessing and handling information in order to conduct official business. In order to mitigate these risks the following objectives have been adopted:

Security Objective	**How we measure**	**How we monitor performance**	**KPI**
Regulatory compliance	Horizon Scanning Internal audit Reviews of legislation for updates: https://www.legislation.gov.uk/browse/uk	Number of open Horizon scanning emails. Number of scanning emails checked vs actioned Number of internal audit findings Number of Data Protection related queries, concerns, requests or questions and whether they were responded to in compliance with GDPR	No sanctions, warnings or fines imposed by ICO No non-conformant findings related to Data Protection, GDPR or other regulations Legal register has a review date within the last 365 days Security accreditations remain current
Protect confidentiality, integrity and availability of Phoenix and customer information	Infrastructure monitoring tooling 24x7 Security Monitoring (IPS/SIEM) Posture Management tooling Vulnerability scanning Penetration testing Backup testing	Number of physical and logical security breaches Number of known open vulnerabilities with available fixes or mitigations Number and impact of reported security incidents Number of high risks identified in pen testing and time to mitigate Success rate of restoration tests	No known data breaches All known patch releases applied within target timeframes 99.9% Service uptime (measured against 24x7x365)* 99.9% Oasis services 99.9% authentication services uptime 99.9% of core network services 99.9% Sage services uptime 99.9% Payroll services uptime 100% Restoration success of all tested backups *excludes planned maintenance windows

Retain accreditation with recognised security standards, namely CE+, PCI DSS, NHS DPST, AEMSP	Internal and external auditing Posture Management tooling	Number of internal and external audit findings and security incidents captured on ISO log Time taken to remediate within standard requirements	100% critical systems (HW & SW) are maintained Patch levels and security definitions are up to date No major non-conformity findings Minor non-conformities are corrected in accordance with target dates Remediation times are within acceptable targets of standard
Foster a strong information security culture	Staff training and awareness campaigns Security notifications or bulletins Number of reported incidents or near misses	Review of completion success ratios Review of time taken to achieve 50% completion Number of security incidents captured on ISO Log	95% completion of annual security training campaigns 50% completion of annual security training completed within 4 weeks of launch Remain under industry average for being Phished over course of FY One focussed All Staff bulletin per FY One security update to TV screens/noticeboards per FY
Suppliers to comply with Phoenix's information security needs	On-boarding due diligence checks and on-going Mainline supplier reviews Internal audit	Number of rejected supplier requestes Number of reported supplier related security incidents Number of suppliers by-passing on-boarding diligence Number of internal audit findings	All Mainline suppliers undergo annual review All onboarded suppliers taken through Phoenix diligence process No known supplier related security breaches No non-conformity findings
All security policies reviewed within a twelve month period	Review of all information security policies & procedures	Tracking of reviewed policies	All live security policies on Hub have an authorised approval date within the last 365 days

Non-compliance with this policy could have a significant effect on the efficient operation of the company and may result in financial loss, an inability to provide necessary services to our customers or the ability to trade.

Policy Compliance

If any user is found to have breached this policy, knowingly or unknowingly, they may be subject to Phoenix disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, please seek advice from the Phoenix HR Manager or any member of the Information Security Committee.

Policy Governance

The following table identifies who within Phoenix is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Information Security Committee
Accountable	Managing Director / Chief Technology Officer
Consulted	Directors, Information Security Committee
Informed	All Employees, Contractual Partners and Third-Party Agents.

Version Control

Author	Version	Date	Description
ISC	1.0	01/07/2015	Original Document
ISC	4.0	25/04/2018	Policy Statement
ISC	5.0	13/09/2018	Full review of policy
ISC	6.0	03/04/2019	Update objectives
ISC	7.0	10/10/2019	Full review of policy
ISC	7.0	12/10/2020	Full review of policy
ISC	8.0	14/11/2021	Update of objectives to include SIEM monitoring
ISC	8.0	17/01/2023	Annual Review – no changes
ISC	8.1	11/07/2023	Objectives added following MRM

Document Approval

Name	Version	Date	Position
Clare Metcalfe	1.0	01/07/2015	Operations Director
Clare Metcalfe	4.0	25/04/2018	Operations Director
Clare Metcalfe	5.0	13/09/2018	Operations Director
Clare Metcalfe	6.0	03/04/2019	Operations Director
Clare Metcalfe	7.0	10/10/2019	Operations Director
Clare Metcalfe	7.0	12/10/2020	Operations Director
Clare Metcalfe	8.0	14/11/2021	Operations Director
Clare Metcalfe	8.0	17/01/2023	Operations Director
Clare Metcalfe	8.1	14/07/2023	Operations Director

Signed: Clare Metcalfe Clare Metcalfe, Operations Director

Dated: 14/07/2023