Information Security Policy

PHX025

Contents

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.

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:

Objective	Measurable Target	Reporting Duration	Reporting Measure
No. 1 Ensure compliance with current laws, regulations, and guidelines	Understand the Acts and Regulations and their applicability	Annually - December	Information Security Committee to review relevant Acts and Regulations and ensure compliance as applicable to the company. Any changes are updated within the ISM section 16.0 Monitored By: ISC Reviewed By: ISC
No.2 Establish controls for protecting company information and information systems against theft, abuse and other forms of harm and loss	100% checks made	Daily	Utilise SIEM tools reporting on Unsuccessful User Logons and Individual User Action. Evidence shown within the reporting tool. Auditing tool to be used for daily checks
No.3 Motivate employees to maintain the responsibility for, ownership of and knowledge about information security, in order to minimize the risk of security incidents	All employees are signed up on the eLearning platform. Mandatory completion of modules by employees in assigned timescales	Quarterly	Utilisation of an eLearning system throughout the company. Data obtained from the eLearning Dashboard and reviewed at quarterly ISC meetings.
No.4 Ensure the protection of personal data (privacy)	100% confidentiality	Weekly for payroll files and continuous for personnel files	Monitoring of all Payroll files by SIEM with alerting on un-authorised access attempts. Evidence shown within the reporting tool.
No.5 Ensure the availability and reliability of the network infrastructure and the services supplied and operated by the company	100% checking of data 97% network availability. Domain access of at least 354 out of 365 days	Daily	Daily Infrastructure Checks including visibility checks on Main Computer room/Power room. Checking all DR, mail, databases, VDI and authentication services. Evidence shown within the reporting tool.

Objective	Measurable Target	Reporting Duration	Reporting Measure
No.6 Ensure that external service providers comply with the company's information security needs and requirements	Checking of relevant supplier's compliance	Annually, and when on-boarded	Technical, Operations and HR Department work with their key suppliers to identify their compliance. Spreadsheet updated in SharePoint/Operations Folder.
No.7 Ensure the physical security	Intruder Alarm - daily Swipe Access Control - monthly Generator Testing and Safety - Twice monthly CCTV Cameras - Weekly Emergency Lighting - monthly	Variety	Swipe System – Admin check weekly to ensure system functioning. Intruder Alarm – onsite readouts. CCTV –
No.8 Continual improvement of the Information Security Management System	More than one amendment made to the policy documents, which have in turn been driven by an improvement made to the system	Ongoing	Review version numbers of policy and procedure documents. Results discussed in minuted ISC meetings

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	2.0	12/11/2015	Update to list of objectives
ISC	3.0	02/12/2015	Update list of objectives and number objectives
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

Document Approval

Name	Version	Date	Position
REDACTED	1.0	01/07/2015	Operations Director
REDACTED	2.0	12/11/2015	Operations Director
REDACTED	3.0	02/12/2015	Operations Director
REDACTED	4.0	25/04/2018	Operations Director
REDACTED	5.0	13/09/2018	Operations Director
REDACTED	6.0	03/04/2019	Operations Director
REDACTED	7.0	10/10/2019	Operations Director
REDACTED	7.0	12/10/2020	Operations Director
REDACTED	8.0	14/11/2021	Operations Director
REDACTED	8.0	17/01/2023	Operations Director

Signed: REDACTED Operations Director

Dated: 17/01/2023