System Access Control Policy

PHX027

Contents

Policy Statement

Phoenix will ensure that all information assets are adequately protected and kept secure during all phases of the employment life cycle of all Phoenix personnel. When applicable this policy will also apply to temporary workers, third party contractors and agents of the Company.

Purpose

Information security is a business-critical requirement that Phoenix has a responsibility to protect. Employees, subcontractors, agents of the company and visitors to the company can all pose a threat to information security and as such must be adequately educated, controlled, and managed to ensure that they have no negative impact on the security of information either unintentionally or intentionally.

This Policy controls the people that have access to information, the processes they follow, and the physical computer equipment used to access them, to ensure that high levels of information confidentiality, integrity and availability are maintained.

The following policy details the basic requirements and responsibilities for the control and management of all phases within the employment cycle at Phoenix regarding information security.

Intended Audience

This document is intended for all employees and interested parties in the information security management system of Phoenix.

Scope

This Policy applies to all aspects of the employee life cycle (all positions) from appointment, through employment, role change and termination.

Pre-Employment

All prospective employees are subject to basic screening before employment is confirmed. If the employee is required to work in a role with secure information, have access to secure information, or to work with equipment that processes secure information, then the company may decide to make additional checks on the individual prior to making a job offer. These checks could include but are not exclusive to the following:

- Identity checks (Passport, driving licence)
- Right to work (Visa if necessary)
- References (if necessary)
- Employment history (CV)
- Qualifications for role suitability (certification, CV)

Any pre-employment checks are conducted by suitably experienced staff or by approved agents of the company. If there are unexplained gaps in employment history and/or inaccuracies in the candidates CV, these will be investigated prior to an offer of employment.

When a job role is more sensitive or is a managerial position that has specific information security responsibilities, these responsibilities will be contained within any role description or within the understanding of the key responsibilities for the position.

Within the employee contract of employment and Company Handbook, terms and conditions include a clear outline with respect to information security stating the implications of breaching the Phoenix Information Security Policy.

Employee Commencement and During Employment

All employees receive an induction at the start of their employment with Phoenix within the first week of employment. This policy deals with the Information Security aspect of the induction process.

The induction provides an introduction to the Information Security Policy and the associated policies relating to generic elements of information security that affect an employee of Phoenix and any specific elements to the new employee's role. All employees are made aware of their basic responsibilities for information security.

Employees are required to sign a confirmation that they have read and understood their responsibilities with regard to information security. All employees are provided with access to the current Information Security policies via the Company Handbook or SharePoint intranet site. Any training that may be required in respect of the individual's role and the Information Security policies is provided during the course of their employment. Phoenix managers are aware of their responsibilities and that of their direct staff in terms of information security and take the necessary steps to ensure that education, awareness and (when required) training is made available. If refresher or update training is required then the HR Manager, with guidance from the IT senior management will identify the requirements and plan this accordingly.

Any contracted third parties, visitors and agents of the company are made aware of and are given guidance to the company's information security requirements before commencement or engagement with Phoenix.

There is a disciplinary process in place to deal with employees who deviate from the procedures, either knowingly or unknowingly, relative to information security. Employees are made aware of

their responsibilities and the disciplinary process at the start of their employment and within their contract of employment.

This disciplinary process can lead to immediate dismissal and further action should illegal actions be involved.

User IT Access

The creation of the User IT Access record by HR is the trigger to the Service Desk department to configure a new user account and associated rights. HR provides details of the new employee's name, job title and line manager which begins the workflow process whereby an e-mail is generated for the Service Desk department who will complete the User IT Access record.

User access is modelled based on the job title of an existing colleague and then the user is added to the relevant AD groups.

Termination of Employment or Change of Employment

The HR department (via the departmental manager) communicate the termination of the employee's contract of employment to the Service Desk department by editing the User IT Access record and entering an end date. This triggers an e-mail for the Service Desk department who then disable the AD account and change the password (strong and complex). HR can contact the Service Desk directly in emergency circumstances.

The departmental manager in conjunction with the HR Manager is responsible for controlling how employees are terminated or re-assigned and therefore also their information security access level. When an employee is terminated or re-assigned all equipment, documents and information appertaining to information security and the role must be returned at the agreed point in time when all physical access rights and privileges are removed or adjusted. It is the responsibility of the departmental manager and the HR Manager to ensure that this is completed in a timely and effective manner in line with the relevant procedure.

Where user requires access to key external systems the user profile is updated. When the user leaves, user profile is disabled, and e-mails forwarded to assigned work colleague.

If a user account has its access level changed this will be authorised by the employee's departmental manager and submitted as a request to the Service Desk. Any changes that require access to another colleague's mail or files also requires permission from the immediate departmental manager or a Director. The access to this resource is temporary and therefore the Service Desk department are responsible for amending access when it's no longer a business requirement.

If a change to user access is required for a job role change then a similar user's AD group membership will be reviewed, and the relevant account will be changed accordingly.

Management of Secret Authentication Information of Users

Users are required to keep any secret authentication information confidential, i.e. their password and the guest wireless network password.

The unlocking of a user account or creation of new account will always require that the user changes their password when they first logon.

Phoenix utilises an AD password policy that ensures strong passwords are used by staff. Passwords must be at least 8 characters long contain both upper and lower case along with a number or special character.

Secure Log-On Auditing

To ensure log on to the company's systems are secure the following are in place:

- CTRL-ALT-DEL is always required
- Incorrect passwords are locked out
- All logins remotely and on the LAN are audited

Password Management System

The passwords for all users are securely stored and follow a best practice password policy as follows:

Policy	**Value**
Keep Password History	Last 5 passwords
Maximum Password Age	91 days
Minimum Password Length	8 characters
Password must meet complexity requirements	True

Use of Privileged Programs

All AD utility-based tools are only restricted to the Service Desk department and authorised personnel as they are members of the Domain Admins AD group.

Version Control

Author	Version	Date	Description
ISC	1.0	01/07/2015	Original
ISC	2.0	08/08/2017	Amendment to max password age
ISC	3.0	19/09/2017	Reviewed / No Change
ISC	4.0	10/10/2019	Reviewed / No Change
ISC	5.0	09/09/2021	Reviewed / No Change
ISC	6.0	02/08/2022	Updated terminology during annual review

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	01/07/2015	Managing Director
Sam Mudd	2.0	08/08/2017	Managing Director
Sam Mudd	3.0	19/09/2017	Managing Director
Sam Mudd	4.0	10/10/2019	Managing Director
Sam Mudd	5.0	09/09/2021	Managing Director
Clare Metcalfe	6.0	30/09/2022	Operations Director

Signed: Clare Metcalfe Clare Metcalfe, Operations Director

Dated: 30/09/2022