System Access Control Procedure

PHX028

Contents

Procedure Statement

Phoenix try to ensure that its Information Security policies are supported by a procedure document. This procedure articulates how the company fulfils its Information Security System Access Policy.

Purpose

This procedure explains how access to data is created and managed for staff and trusted third parties at Phoenix. It identifies how the company implements its System Access Control Policy.

The procedure gives details on the responsibilities for the control and management of access to company data during all phases of the employment cycle at Phoenix as it appertains to information security. The procedure ensures that staff and third parties have access to the data that is required for them to fulfil their role at Phoenix.

Intended Audience

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

Scope

This procedure only supports the requirements contained in the System Access Control Policy. It contains guidance on management of company data access for employees, ex-employees and trusted third parties. Throughout the procedure the employee and third parties are referred to as workers.

New Starter Procedure

Background

The HR Department inform the Service Desk Department via the User IT Access folder within SharePoint. This records the access rights that a worker needs to fulfil their role. The Service Desk Department own the User IT record, which in conjunction with the Client Asset Log verifies what hardware, software, and data an employee needs to access.

This procedure covers how Active Directory (AD), mail, telephone, device, and mobile data is set up for an employee. The User IT record shows the access a user has to company information at any point in time.

Create User IT record

The HR Department populate the User IT record. This contains the basic information of:

- Name
- Job Title
- Department
- Line Manager
- Mobile
- Start date

Create AD user account

The Service Desk Department create the user account in the user identity system as per the new user record in format first name-last name.

Configure AD user account

The user is granted minimum permissions and access is added as requested by way of authorisation from a manager.

- The device's asset tag is used as the computer name and added to AD

The fuller asset information is recorded separately by the Operations Department in the Client Asset Log. The Organisation Units (OU) locations are recorded for the user and the computer.

Configure user device

Each user device (tablet, laptop, or PC) is configured using a standard build which has security:

- Install Windows operating system using Windows Deployment Server
- Install all Windows updates
- Join the device to the identity system
- Install Anti-virus (deployed automatically once device added to the domain)
- Install the encryption client where applicable

Deploy business applications

Each user device (tablet, laptop, or PC) is configured using the same base applications:

Other staff use a thin client with a standard Windows virtual desktop which already has all line business applications installed.

All applications are tested by a Service Desk engineer and all business applications are visited during the employee's technical induction.

Configure user access

The AD access rights are configured based on the manager's request. The engineer tests the user logon and access to all applications.

Configure telephone access

The user telephony access is created based on a team membership. A number is allocated based on availability.

Configure mobile access

A company mobile is configured to limit application usage:

- Add user account to Wireless Devices AD group
- Configure device Exchange active synchronisation
- Check user's speed dial properties on the Telephone system for the newly allocated mobile
- Install the Mobile Device Management configuration profile

Leaver Procedure

Background

The HR Department inform the Service Desk Manager via e-mail or telephone that an employee is leaving so that user data is secured. If the user is being placed on garden leave the Service Desk Manager will liaise with the line manager and HR Manager as to the data access required. Each garden leave case may differ, the access change is recorded on the User IT record, but the end date omitted.

Once employment is terminated, the user password is changed immediately, and the account is disabled. The user device is retrieved and returned to Service Desk by the HR Department.

The Leavers Process is documented in Service Desk Leavers Knowledge Base Guide. This information is maintained and developed by the Service Desk Team.

Version Control

Author	Version	Date	Description
ISC	1.0	01/07/2015	Original Document
ISC	2.0	19/09/2018	Annual Review
ISC	3.0	10/10/2019	Annual Review
ISC	4.0	02/08/2022	Content Update

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	01/07/2015	Managing Director
Sam Mudd	2.0	19/09/2018	Managing Director
Sam Mudd	3.0	10/10/2019	Managing Director
Clare Metcalfe	4.0	30/09/2022	Operations Director

Signed: Clare Metcalfe Clare Metcalfe, Operations Director

Dated: 30/09/2022