Encryption and Cryptographic Controls Policy

PHX039

Contents

Intended Audience

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

Policy Statement

Phoenix values the importance of protecting business critical data from unauthorised access, disclosure, or loss. Cryptographic controls are therefore used to provide secure keys that protect data stored on devices. These controls also provide the control to secure the data being passed to a third party. This policy details the management and usage of cryptographic controls to provide security to information that is at risk. The disk encryption in use to cover Blenheim House mobile devices is AES 256-bit

Scope

Information security is a business-critical requirement that Phoenix Software Limited has a responsibility to protect.

As the company transacts with its customers on-line it is important that all data that is passed between third parties and Phoenix is secure.

All web traffic transported between its customers will use SSL with a 256-bit encryption key.

It is important that staff have a device which uses encryption, where possible, that maintains the confidentiality of that device if the digital media was removed from the device itself or the laptop was accessed by an unauthorised person.

The policy details the management of the keys that keep transmitted data safe, their algorithms, key lengths, and usage according to industry best practice.

Method

All Blenheim House laptops have been encrypted with full disk encryption using AES 256-bit encryption. This utilises the Windows BitLocker Drive Encryption functionality.

The end user will usually utilise a TPM chip on their device.

Once the build process for the laptop is completed the device encryption is performed via the BitLocker program on the laptop, as the process is completed the key that is used to encrypt the boot volume is synchronised to the computer object in the Phoenix Active Directory.

This key itself is created by BitLocker and stored as a backup in the AD database. The Service Desk can recover these keys in the event that the end user has no access to the recovery key. The recovery of the key to decrypt the drive is performed by accessing AD which is only accessible by Service Desk staff.

Controls

The Phoenix Active Directory which manages the encryption of all laptops is accessible by designated security officers only, who are members of the Service Desk team. These staff are the only individuals who can access the keys that are valid to gain access to any encrypted devices. If the end user needs to recover the device as they have no record of their recovery key, they can contact the Service Desk who can assist in performing a recovery of the encrypted hard drive.

Access to removable storage devices is denied, blocking both read and write access to any such devices. Alerting of USB access is carried out on a real-time basis by an anti-virus client installed on all company machines and monitored via SOC.

Employees shall not store confidential or internal use data on removable media (SD-card, USB, CD-ROM etc.)

Version Control

Author	Version	Date	Description
ISC	1.0	04/12/2015	Original Document
ISC	2.0	09/12/2015	Confidential Data shall not be stored on removable able
ISC	3.0	09/03/2016	Cryptographic keys shall be stored in AD
ISC	4.0	19/09/2018	Annual Review
ISC	5.0	01/04/2020	Annual Review
ISC	5.0	02/04/2021	Annual Review
ISC	6.0	02/08/2022	Content Update

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	04/12/2015	Managing Director
Sam Mudd	2.0	09/12/2015	Managing Director
Sam Mudd	3.0	09/03/2016	Managing Director
Sam Mudd	4.0	19/09/2018	Managing Director
Sam Mudd	5.0	01/04/2020	Managing Director
Sam Mudd	5.0	02/04/2021	Managing Director
Clare Metcalfe	6.0	30/09/2022	Operations Director

Signed: Clare Metcalfe Clare Metcalfe, Operations Director

Dated: 30/09/2022