Vulnerability and Patching Policy

PHX040

Contents

Intended Audience

This policy applies to all members of staff and third parties that access assets owned by Phoenix Software Ltd.

Purpose

The purpose of this policy is to ensure Phoenix IT infrastructure and systems are maintained and running on the most recent updates and patches. It is important that vulnerabilities within the IT infrastructure are kept to an absolute minimum to maximise the confidentiality, integrity and availability of Phoenix IT systems and the data it holds. This policy will outline the approach for regular patching and vulnerability management to ensure compliance.

Scope

This policy applies to all Phoenix owned IT Infrastructure, systems, client devices, mobile phones, appliances hosted in Phoenix data centres, 3rd party datacentres or public cloud and where contractually agreed – customer environments/systems.

Policy Statement

- Maintenance schedule will be recorded within the Phoenix IT Service Management tool where completion will be tracked.
- Reminders for maintenance jobs sent to the ITSM tool which creates a support ticket
- Support ticket will be used to track the progress of the maintenance jobs through to completion
- System owners will complete or co-ordinate the maintenance jobs
- Patching routines should be automated when possible
- As best possible patching should be completed in phases across the estate to mitigate any potential impact
- Patching routines will be documented
- Penetration tests to take place yearly or after major changes
- Ongoing vulnerability scanning against perimeter network via Digital Shadows
- Any vulnerabilities discovered must have a support ticket created and actioned through to completion as soon as reasonably possible
- When reasonably possible if downtime is required then patching should take place outside of core business hours
- Phoenix will use the common vulnerability scoring system (CVSS) to assess vulnerabilities
- Vulnerabilities that cannot be remediated will be added to the risk register
- When new services are moved into production, they must be running the latest supported versions prior to their release

- Incident and problem management may result in a need for patches and updates to be applied
- Patches which are installed manually are subject to change management taking into consideration testing and rollback when possible
- Patching requirements for customer environments will be detailed in individual contracts.
- Patching for customer environments under professional services will be subject to the customers change management procedures throughout the project
- Patching for customer environments under managed services will be subject to the Phoenix IT Service Desk change management process and approved by nominated customer change authority.
- Exceptions to this policy require formal Director approval

Ownership

Asset	**Owner**
Network Switches	Infrastructure/Systems Team
Server Firmware	Infrastructure/Systems Team
Hypervisors	Infrastructure/Systems Team
Windows Server Operating Systems	Infrastructure/Systems Team
Windows Client Operating Systems	Infrastructure/Systems Team
Wireless Infrastructure	Infrastructure/Systems Team
Storage Infrastructure	Infrastructure/Systems Team
License Dashboard Customer Environment	License Dashboard Technical Team
License Dashboard Applications	License Dashboard Development Team
Oasis Business Applications	Phoenix Systems Development Team
Dynamics 365	Phoenix Systems Development Team
Third Party Systems	Third Party Owners
All other Phoenix applications	Infrastructure/Systems Team

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 Management 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	Governance Manager
Accountable	Managing Director / Operations Director
Consulted	Directors, Service Management Committee
Informed	All Employees, Contractual Partners, and Third-Party Agents.

Review and Revision

This policy is reviewed as it is deemed appropriate, but no less frequently than every 12 months. Policy review will be undertaken by the ISMS with any subsequent changes authorised by the Operations Director.

Version Control

Author	Version	Date	Description
ISC	1.0	04/08/2015	Original
ISC	1.0	14/06/2016	Annual Review
ISC	2.0	04/04/2017	Content Upgrade
ISC	2.0	25/09/2018	Annual Review
ISC	3.0	04/04/2020	Annual Review
ISC	3.0	05/04/2021	Annual Review
ISC	4.0	09/08/2022	Content Update

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	04/08/2015	Managing Director
Sam Mudd	1.0	14/06/2016	Managing Director
Sam Mudd	2.0	04/04/2017	Managing Director
Sam Mudd	2.0	25/09/2018	Managing Director
Sam Mudd	3.0	04/04/2020	Managing Director
Sam Mudd	3.0	05/04/2021	Managing Director
Clare Metcalfe	4.0	30/09/2022	Operations Director

Signed: Clare Metcalfe Clare Metcalfe, Operations Director

Dated: 30/09/2022