

Vulnerability Management Policy

Reference: PCI POL 6.1

DocumentKits Issue No: 1.1

Organisation Issue No:

DocumentKits Issue Date: 29/06/2020

Organisation Issue Date:

1. Scope

All of Organisation Name's operational software is covered in the scope of this policy, including external support.

2. Responsibilities

2.1 The Head of Systems Testing is responsible for testing operational software.

2.2 The Head of Systems Testing is responsible for identifying new security vulnerabilities, including the use of outside sources for security vulnerability information, and updating the system configuration standards accordingly.

2.3 The Head of IT (CIO) is responsible for the operational (live) environment.

2.4 The Change Manager is responsible for managing the transfer of software from development to test to operational environments.

2.5 The Change Manager is responsible for the central storage of system documentation.

2.6 The Project Manager is responsible for the security of any given development project.

2.7 The
"software developers"

are responsible for reporting identified vulnerabilities.

3. Requirements

3.1 Organisation Name's operational software is listed in the asset and each item of

operational software has an identified Owners, who is the trained administrator of that item of software. Only the Owners may perform software updates, and then only with the prior authorisation of the Head of IT (CIO) after the completion of satisfactory testing.

"Set out how this authorisation should be provided – email or some other documentation."

3.2 The Head of IT (CIO) maintains a configuration control schedule for all operational software.

"Identify here how it links to the asset inventory and to the Change Manager's method of storing system documentation."

"An audit log for all updates to operational program libraries is maintained."

3.3 Software change management is carried out in line with an approved procedure. Change management must be documented on a [Change Request Form](#) and includes: Documentation of impact, management sign-off by authorised parties, testing of operational functionality and back-out procedures.

3.4 Previous versions of operational software are retained as a contingency.

"for how long, where, under whose control, and with what additional information?"

3.5 All system components (including payment applications) and software have the latest vendor-supplied security patches installed within 1 month of release; critical security patches are installed within one month of release.

3.6 Physical or logical access is only given to suppliers and in line with an approved procedure.

"under what conditions/against what criteria?"

3.7 New security vulnerabilities are identified by means of monitoring CVE and bugtraq releases, and by means of regular penetration testing and ASV scanning. Vulnerabilities are ranked on the basis of risk to Organisation Name using this policy and the industry standard CVSS rating scheme. Any external vulnerability that has a CVSS base score of 4.0 or above is classed as a critical vulnerability. Internal vulnerabilities should be assessed in accordance with the risk methodology in use and, at a minimum, identify all vulnerabilities considered to be a 'high risk' to the environment. In addition to the risk

ranking, vulnerabilities may be considered 'critical' if they pose an imminent threat to the environment, impact critical systems and/or would result in a potential compromise if not addressed.

<< 3.8 – 3.11 removed for sample purposes >>

Document Owner and Approval

The Head of IT (CIO) is the owner of this document and is responsible for keeping it up to date.

The current version of this document is available to

"Specify which members of staff this document is intended for"

and is published

"Describe the location(s) – electronic and physical – where this document is available"

Its approval status can be viewed in the [Master List of Document Approval](#).