ICT Patch Management Policy

1. Scope

This policy applies to all software, servers, desktops, firewalls, switches, laptops, SANS and cloud environments owned or operated by the Group hereinafter referred to as HomeChoice.

2. Purpose

The policy aims to reduce system vulnerabilities and to enhance and repair application functionality.

3. Policy

3.1 Vulnerability assessment and system patching will only be performed by the designated infrastructure teams.

3.2 All server, desktop, firewall, switch, SAN and laptop system, including all hardware and software components must be accurately listed in the ICT department asset inventory.

3.3 HomeChoice's system will be scanned for vulnerabilities with the following frequencies:

- A quick scan is performed on a daily basis and a full scan is performed weekly to Windows servers, desktop and laptops.
- Firewall signature databases are constantly updated in real time.

3.4 The applicable software and hardware vendors will be acknowledged as the only authorities and authors of patches against new system vulnerabilities and general improvements. These sources must be monitored by assigned IT personnel on an ongoing basis.

3.5 Each vulnerability alert and patch release must be checked against existing HomeChoice systems and service prior to taking any action in order to avoid unnecessary patching.

3.6 All patches must be tested prior to full implementation since patches may have unforeseen side effects. The order of patching of servers must be in the following order Development, QA and Production.

3.7 The decision to apply a patch and the timeframe must be done following the guidelines presented in the patch priority matrix.

3.8 New servers, desktops, laptops, switches, SANS, firewalls and software must be fully patched as per matrix requirements before coming online in order to limit the introduction of risk.

3.9 A back out plan that allows safe restoration of systems to their pre-patch state must be devised and documented prior to any patch rollout in the event that the patch has unforeseen effects.

3.10 All patch changes will be presented and must comply with the Change Advisory Board requirements.

3.11 Internal reviews will be performed bi-annually to ensure that patches have been applied as required and are functioning as expected.

4. Patch Priorities

4.1 **High Priority** – Patches that could cause significant loss or degradation of business services if exploited or not implemented immediately.

4.2 **Moderate Priority** – Patches that address non-critical or non-security related bugs.

4.3 **Low Priority** – Patches such as service pack or update rollups that have been tested extensively and typically replace an installed version of a product with a newer version of the same product.

5. Patch Matrix

5.1 Windows Environment

5.1.1 Patch priority represents all system infrastructure running Windows environment at HomeChoice, their relative priority for patching and timeframes with which patches must be applied:

5.1.2 **Dev Cycle**: is applicable to development and staging servers which are patched and rebooted on the first weekend (Saturday) of each month.

5.1.3 **Prod Cycle**: is applied to all business-critical servers (excluding priority cycle) which are patched with the latest cumulative patch and rebooted every second weekend of each month.

5.1.4 **Priority Cycle**: is for business-critical servers which are patched with the latest available cumulative patch and rebooted on the third weekend of the month.

5.1.5 **Day Cycle**: Servers that are patched and rebooted every third Wednesday during the day

5.1.6 **Emergency Cycle**: Day zero updates i.e. wannacry will be updated on the day of release.

5.1.7 As business requires sprints to be released every second week due to continuous product development, certain instances will occur where, patch updates will roll over to the next cycle period.

5.2 Database Environment (SQL)

5.2.1 Due to critical business impact that databases have on the overall business operations both SQL & MySQL patch updates will only occur when the following is applicable:

- Identified vulnerability has a material impact on our database environment.
- Likelihood of such vulnerability be exploited exists.
- Uptime or production impact.

5.3 Open Source Environment

5.3.1 The following Patch priority represents all infrastructure running on the Linux environment at HomeChoice, the relative priority for patching and timeframes within which the patches must be applied:

- **Development**: Patch updates may occur continuously (automated) with no prior warning. There is some infrastructure that is listed on the exclusion list i.e. .NetCore and NGINX which is only patched manually when a security warning is received via the landscape software.

- **Production**: In extreme cases, critical security updates could be updated immediately otherwise patch updates will happen on a bi-weekly basis. An exclusion list process also applies here. Applying patch updates must follow the formal CAB process.

5.4 Telephony Environment

5.4.1 Avaya & Asterisk – These environments are managed by independent third-party service providers. An update report along with recommendations are presented to ICT management indicating the current statuses of the application, operating system (OS) and database (DB) versions monthly. Any change to the environment will follow the CAB process.

6. Breach of Policy

Any failure to comply with this policy may be subject to disciplinary action up to and including termination of employment.

7. Breach of Policy

Any exceptions to the policy must be approved by the Infosec committee in advance.

8. Version control

This is a non-contractual policy, and as such HomeChoice reserves the right to modify this policy at any time. Reasonable notice of any changes will be provided. Reasons for any modification may include employment legislation or other guideline changes.

Document title	ICT Patch Management Policy
Version number	V1
Author of document	Bernard Van Der Merwe
Document expert	Bernard Van Der Merwe
Department	ICT
Authorised date	27 June 2018
Authorising authority (pre-approval)	Dirk Oberholster
Authorising authority (final approval)	HomeChoice (Pty) Ltd Board
Date first published to intranet	30 June 2018