**Process Document - 2**

**Patch Management**

|  |  |
| --- | --- |
| **Document Control Sheet** | |
| **For Airtel Money Environment only** | |
| Document Name | Patch Management Process |
| Document Owner | Venkatachal Hegde |
| Effective Date | 01-04-2013 |
| Review Date | 16-03-2013 |
| Review Remarks |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document Version Control** | | | | |
| **Version** | **Date** | **Prepared By** | **Reviewed By** | **Approved By** |
| 1.0 | 28-02-2013 |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1. Process Overview 3](#_Toc349645226)

[2. Security Patch Management Process 5](#_Toc349645227)

[3. Roles and Responsibilities 7](#_Toc349645228)

[4. Control Points 9](#_Toc349645229)

[5. Patch Reports and Dashboards 10](#_Toc349645230)

1. **Process Overview**
2. **Description and Scope**

Patches provide a means to update software without having to upgrade to a new operating system or application version. Patches are used to repair defects and to add or change software features. As with most software environments, patches are part of routine administration for any System Environment.

This section provides the scope of the process and informs about pre-requisites, retaining artifacts and compliance for security patch management.

This document presents a systematic approach for identifying and installing necessary security patches or otherwise mitigating specific problems with respect to OS /DB/App with reference to Airtel Money Environment. The scope of this document is limited to Airtel Money Environment.

1. Critical To Quality Statement for the process

SLA to be reported is >98%

Applicable Patches = (Total Patches) — (Not Applicable + SOD’s + Not Required+ Downtime not provided)

1. Patch Management parameters to be reported

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. No.** | **Check** | **Definition** | **Measurement** | **Frequency** |
| 1. | Patch implementation score |  | 98% | Monthly |
| 2. | Applicable Patches | (Total Patches) — (Not Applicable +SODs + Not required + Down time not provided | NA | Monthly |
| 3. | Overdue Patches | Patches which have not been applied according to the implementation Schedule as agreed with the customer | NA | Monthly |

1. Retaining Artifacts

The artifacts of complete and timely Process execution must be retained according to instructions given within the Process control points for audit trail purposes.

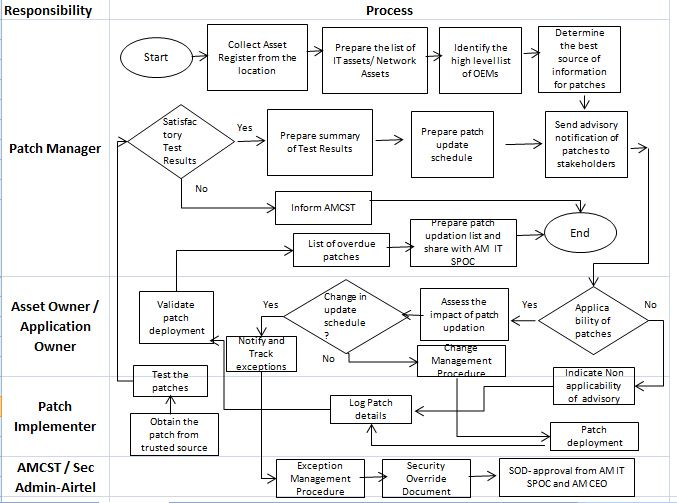
1. Measurements

|  |  |  |
| --- | --- | --- |
| Steps | Measurement |  |
| Definition | Target |
| 1. | Patch Advisories | As received |
| 2. | Timelines for Implementation | Recommended Implementation Schedule timelines:  High Severity. - 50 Days  Medium Severity - 60 Days  Low Severity - 90 Days |

1. Risk Statement

Non-implementation security fix and patch for all the software components like OS, DB, App and other sub-systems of the servers gives exposure for exploitation of the security weakness and would allow unauthorized breach of security environment.

1. **Security Patch Management Process**



**Security patch management process workflow**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl. No.** | **Activity** | **Responsibility** | **Output** | **Internal SLAs/ Performance Criteria** |
| 1 | Acquire the latest copy of the Airtel Money Asset Register | Patch Manager | Latest patch released by vendor | Turnaround time to discover a patch released by a vendor (alert) and assign priority |
| 2 | Determine the best source of information about Patches applicable to platform/ Applications/ Network devices. | Patch Manager | Patch Source | NIL |
| 3 | Prepare an advisory of all patches pertaining to the list of all platforms/ Applications/ Technical-Network devices and send it to Patch Implementer, Asset Owner | Patch Manager | Patch Criticality determined | NIL |
| 4 | Determine if patch testing in the test server is successful. | Patch Implementer | Test results, | Turnaround time for critical patch testing and deployment without planned downtime |
| Patch updation report |
| 5 | Discard patch updation for patch not successfully tested in test server. | Patch Implementer | Patch Updation Schedule | NIL |
| 6 | Raise a change request in Service manager tool and follow change management procedure for patches to be deployed | Asset Owner/ Application Owners | Closed change request with all approvals | NIL |
| 7 | Validate the patch updation after patch deployment and provide a list of overdue patches with respect to IT asset/ Technical-Network assets. | Asset Owner / Application Owners | List of servers where latest patch was not deployed. | NIL |
| 8 | Ensure patches are deployed on servers which were not updated before | Patch Implementer | Patch Updating Report | No of incidents raised due to unsuccessful deployment of patch. |
| 9 | Review the list of overdue patches corresponding to each IT asset/Network asset and direct the asset owner/ application owner, | Patch Manager | Patch deployed on all servers successfully | NIL |
| 10 | For the systems where patch could not be deployed, Follow Exception Management Procedure | AMCST/ Sec Admin-Airtel | Security Override Document |  |
| 11 | SOD Approval | AMCST / AM IT SPOC + AM CEO | Get the SOD approval from AM IT SPOC and AM CEO |  |

1. **Roles and Responsibilities**

This section describes responsibilities of those involved in delivering or supporting the Patch Management Process. Responsibilities include but are not limited to those listed for each role.

Roles are meant as logical groupings of tasks. They are not meant to match any particular Service Delivery organizational structure:

• Several roles might be performed by the same individual.

• A role may be split up among several individuals.

Key responsibilities are as below:-

1. Patch Manager: Comviva Airtel Money Security Team member
2. Patch Implementer: Comviva Ops team member (L1/ L2)
   1. **Patch Implementer**

The Patch Implementor responsible for:

* Monitor and governing the Security Patch Management Process for Airtel Money Environment.
* Writing and maintaining of the local patch procedures and work instructions following the framework given in the Patch Management Process
* Maintaining a list of systems/platforms/middleware as per the environment.
* Testing and Implementing the patches as per the schedule.
* Regular validation and subscription of systems/platforms/middleware/ database according to available environment.
* Maintaining list of relevant focal points and updating the same for patch notifications.
* Create a monthly patch dashboard from the patch reports.
* Supporting Patch Management process
* Storing artifacts for actions completed.
* Monitoring for Security Patch alerts for requested software
* Assigning severity classification (High/ Medium /Low) where appropriate.
* Maintaining a central repository with Security Patch information.
  1. **Patch Manager**

The Patch Manager is responsible for:

* Receiving Security Patch alerts for specific platforms.
* Creating Master Security Patch records manually / (in the Patch Management Tool for the alerts received.)
* Notifying Patch Implementor of Security Patch received, (if not done automatically by the Patch Management Tool)
* Conducting periodic verification of received patches against opened Master Security Patches
* Collecting and storing artifacts of done actions for audit trail purposes
  1. **AMCST**

The Compliance Team is responsible for

* Support of implementation of the security policy.
* Receiving, reviewing and address Patch implementation date extensions
* Contacting the requester in case additional artifacts are required

1. **Control Points**

Control Points are activities identified within the processes that support effective execution of the process.

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Point** | **Risk** | **Process Flow Steps** | **Control Requirement.** |
| 1 | Invalid list of  Systems /  Platforms | Maintain list of Systems, Platforms, Middleware | The list of systems platforms / middle ware needs to be maintained and a monitoring service provider selected for all on the list. This activity needs to be done quarterly. |
| 2 | Non-compliance to policy requirements | Determine Monitoring Requirements as per policy | Any software in Airtel Money Environment may be in scope for patching; therefore it needs to be controlled. |
| 3 | Patch tracking noncompliance | Create Master Patch | A unique patch record (out of the Master Patch record) needs to be created for the environment with notification to the Monitor. |

1. **Patch Reports and Dashboards**

Asset Register

Patch Management Advisory

Patch Management Tracksheet

****

Patch Report will have three sub sections.

First section will be for Patch Availability and Applicability Report which will detail the analysis of the Patches and its suitability to the environment. This will have the impact assessment and Roll back plan details in case the patch is approved to be deployed.

Second section will have Details of Patch Deployment in Test Environment and analysis of System Functionality Post Deployment.

Third section will have the final details of Patch Deployment in Production Environment.

Annexure :

1. Contact Details :

|  |  |  |
| --- | --- | --- |
|  | **Contact Person** | **Contact details** |
| Patch Implementer () |  |  |
| Business Head  –Airtel Money () |  |  |
|  |  |  |