**Process Document - 20**

**Preventive Maintenance**

22.04.2013

|  |  |
| --- | --- |
| **Document Control Sheet** | |
| **For Airtel Money Environment only** | |
| Document Name | Preventive Maintenance Process |
| Document Owner |  |
| Effective Date |  |
| Review Date |  |
| Review Remarks |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document Version Control** | | | | |
| **Version** | **Date** | **Prepared By** | **Reviewed By** | **Approved By** |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1. Process Overview 3](#_Toc355233060)

[2. Process Activities 3](#_Toc355233061)

[3. Process Inputs and Outputs 5](#_Toc355233062)

[4. Process KPIs and Reports 6](#_Toc355233063)

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

This document describes the process to be followed for the basic hygiene check, monitoring the hardware, OS, utilization of CPU, memory, hard disk, processes, logs, interfaces, deploying the upgrades/patches, trend analysis.

The process will be applicable for :

1. Application Software
2. Hardware / Servers
3. System Software
4. Network Devices

Preventive maintenance is defined as a procedure of inspecting, testing and reconditioning a system at regular intervals according to specific instructions, intended to prevent failures in service or retard deterioration.

The objective of Preventive Maintenance process is to undertake proactive measures so as to ensure the uninterrupted availability of the Airtel Money environment.

1. **Process Activities**

Preventive Maintenance is the process by which activities like basic hygiene check, monitoring the hardware, OS, utilization of CPU, memory, hard disk, processes, logs, interfaces, deploying the upgrades/patches, trend analysis carried out to ensure the uninterrupted availability of the service.

Depicted below are the activities under Preventive Maintenance process:

* Basic Hygiene Check
* Hardware Monitoring
* OS Monitoring
* CPU Utilization
* Memory Utilization
* Hard Disk Utilization
* Monitoring of Processes
* Monitoring of Logs
* Monitoring of Interfaces
* Recording the history of events, logs
* Trend Analysis
* Patch Deployment
* Capacity Management

**Basic Hygiene Check**

The Basic Hygiene Management process consists of the tasks and policies used to check, verify and ensure the compliance for Information Security assests.

The Basic Hygiene Management includes the following capabilities:

* Check and comply the servers for each applicable advisory point
* Ensure the integrity of the data related to the Basic Hygiene Management process.

**Hardware Monitoring**

This process involves proactively monitoring the health of the hardware components like server, CPU, memory, hard disk to ensure that all the systems are running fine all the time.

**OS Monitoring**

This process involves mointoring the parameters of Operating System and middleware components to catch any unexpected behavior or degradation in performance.

**CPU Utilization**

Utilization of CPU by different processes and total CPU utilization is monitored. Alarm is raised whenever the utilization reaches pre-defined upper limit.

**Memory Utilization**

Utilization of memeory ( RAM) by different processes and total CPU utilization is monitored. Alarm is raised whenever the utilization reaches pre-defined upper limit.

**Hard Disk Utilization**

Utilization of Hard Disk and available free space is monitored. Alarm is raised whenever the utilization reaches pre-defined upper limit

**Monitoring of Processes**

All the processes are monitored to make sure that they are in the desired stae all the time. Also the CPU and Memory utilization by each process is monitored and Alarm is raised whenever the utilization reaches pre-defined upper limit.

**Monitoring of Logs**

Application logs are continuously scanned to search for specific pre-defined keywords which indicate some undesired behavior with the application. Alarm is raised whenever the utilization reaches pre-defined upper limit.

**Monitoring of Interfaces**

All the incoming and outgoing interfaces of the application are monitored to make sure that they are working fine all the time.

**Recording the history of events, logs.**

A pre-defined set of events and logs are recorded and maintained for a pre-defined duration. These events and logs are analyzed for doing the Trend Analysis.

**Trend Analysis**.

The recorded events and logs are analyzed. Any unexpected behavior or degradation in performance with any components is analyzed and corrective action is taken to prevent any failure.

**Patch Deployment**

Identified patches for OS, middleware, firmware are deployed to prevent any failure with the system.

**Capacity management**

CPU, Memory and Hard Disk Utilization are analyzed and correcive actions are taken to avoid any failure with the system.

1. **Process Inputs and Outputs**

**Inputs**:

The inputs required for Preventive Maintenance Process are :

* Monitoring Logs
* Trend Analysis Reports
* Application Logs
* Security Patches

**Activities:**

* Recording the history of events and logs
* Analyzing the trebds and logs
* Identifying the problem areas
* Identifying the preventive measures to be taken
* Deploying the action plan

**Outputs :**

* Implementation / roll-back plan executed
* Normal Business operation restored

1. **Process KPIs and Reports**

Process Owner needs to provide ongoing reporting around the KPIs and process-related metrics and trends that indicate the health of the pprocess to the SM and IT management on a regular basis as part of the process reviews and continuous improvement plans.

Below are some of the Key Perfromance Indicators (KPI) and reports which come out through this process.

* Number of Hygiene Checks – carried out to check the system health
* System Monitoring Report – Capture the monitoring of OS, Memory, Harwdare, Logs, Processes, Interfaces
* System Utilization Report – Capture Utilization of Memory, CPU, Hard Disk.
* Trend Analysis Report –Analysis carried out on recorded events and logs.
* Number of Security Patches deployed.