**Process Document - 3**

**Malware Code Control**

|  |  |
| --- | --- |
| **Document Control Sheet** | |
| **For Airtel Money Environment only** | |
| Document Name | Malware Code Control |
| 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. Introduction 3](#_Toc349560304)

[2. Malware Code Management Process 3](#_Toc349560305)

[3. Malware Code Management Procedure 4](#_Toc349560306)

[4. Roles & Responsibilities 6](#_Toc349560307)

[5. Malware Control Management Reports 7](#_Toc349560308)

[6. Performance Metrics and Benchmarks 7](#_Toc349560309)

[6.1 KPI 7](#_Toc349560310)

[6.2 Vendor SLAs 8](#_Toc349560311)

1. **Process Overview**

The Malware code management process document provides for the scope of the anti-malware management activity, the procedure to control malware code, roles and responsibilities and the KPIs involved in the process.

The objective of the Malware code management process is to detect and determine Malware threats and provide effective Malware outbreak prevention and recovery controls against malicious code.

1. **Definition and Scope**

The scope of the Malware code management process extends to the Airtel Money environment.

The Malware software programs like viruses, worms, Trojans etc. can cause considerable damage to information & IT assets of an organization. Malware Code Management process will provide a proper framework of safeguards and, procedures to control this severe threat to the Airtel Money environment..

The malware code management activity includes the following:

* Detect and manage malware related incidents, issues and alerts
* Ensure the anti-malware server update the Malware signature timely for subsequent updating to systems

The process provides for proactive malware prevention and malware outbreak management process

**Definitions**

Malware - Software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used to represent a variety of forms of hostile, intrusive, or annoying software or program code.

Threat agent - The person or process attacking a system by exploiting its vulnerabilities to violate confidentiality, integrity and availability.

Attack - A threat agent attempting to take advantage of vulnerabilities for unexpected/malicious purposes.

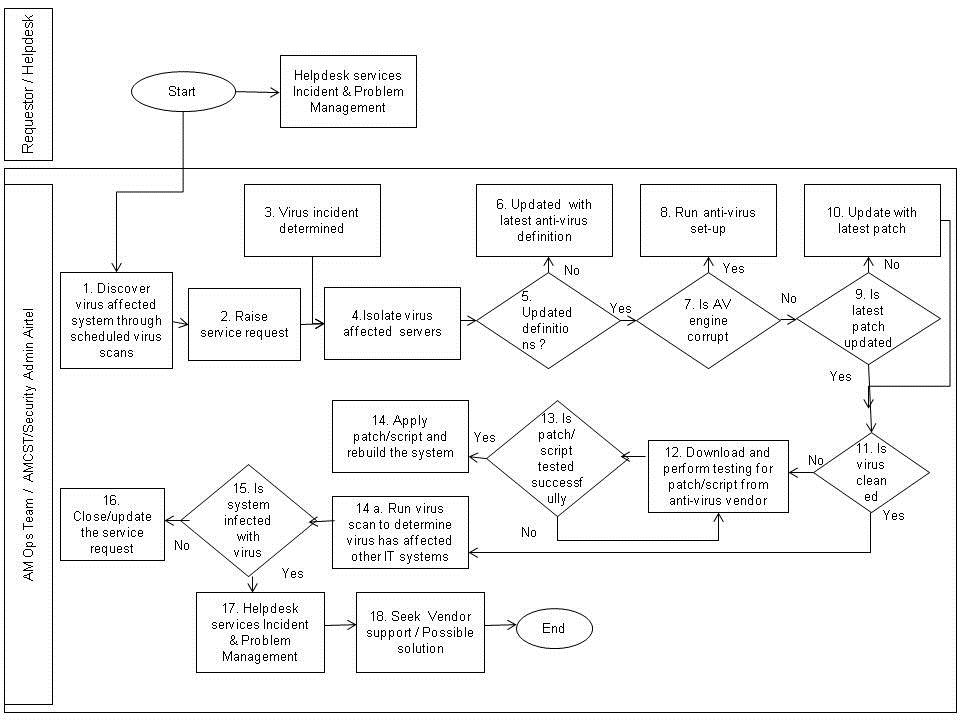
**Dependency**

The following procedure should be referred to wherever applicable in Malware Code Management Procedure:

* Incident Management Procedure
* Patch Management Procedure
* Problem Management Procedure

1. **Malware Code Control Procedure**

**3.1 Process Flow Diagram**



**3.2 Process Flow Steps**

The following table lists down the set of activities performed as part of the Malware code control procedure:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl. No.** | **Activity** | **Responsibility** | **Output** | **Internal SLAs/ Performance Criteria** |
| 1 | Virus alert detected on systems through scheduled virus scans | AM Ops Team | List of systems affected by virus | Turnaround time to test virus definition released and deploy on distribution servers |
| 2 | Raise a service request | AM Ops Team | NIL | NIL |
| Helpdesk |
| 3 | Virus activity is determined through incident and problem management process | AMCST/AM Ops Team | List of systems affected by virus | NIL |
| 4 | Isolate the affected system from the network to stop spreading of virus. | AM Ops Team | Isolation of systems | NIL |
| 5 | Determine whether the affected IT system have latest anti-virus definition | AM Ops Team | Latest virus definitions on systems | NIL |
| 6 | If systems is not updated with latest anti-virus definition downloading latest virus definition and update on the systems. | AM Ops Team | Latest virus definition updated on systems | NIL |
| 7 | Determine whether the affected systems has anti-virus engine corrupted | AM Ops Team | Identification of systems with Anti-virus engine corrupted. | NIL |
| 8 | Run anti-virus setup and install a fresh copy of anti-virus engine | AM Ops Team | Install latest anti-virus engine copy on the affected systems | NIL |
| 9 | Determine whether the affected systems does not have latest patch definition | AM Ops Team | Identification of systems with latest patch not updated. | NIL |
| 10 | Update affected systems with latest patch | AM Ops Team | systems updated with latest patch | NIL |
| 11 | Determine if the affected systems is cleaned from virus | AM Ops Team | Determine whether the systems is cleaned from affected virus | NIL |
| 12 | If the virus still exists check with the anti-virus vendor for patch/script available. If available download and test the latest patch. | AM Ops Team | Perform testing of the patch/script provided by the anti-virus vendor | NIL |
| 13 | Determine if the patch/script is tested successfully in test server | AM Ops Team | Perform testing of the patch/script provided by the anti-virus vendor | NIL |
| 14 | After testing the patch/script successfully in test server apply the patch/script on the affected systems Close/Update the service request | AM Ops Team | Apply successfully tested patch and rebuilt the systems | NIL |
| 14a | Run anti-virus scan on the entire systems to determine whether virus has been affected on other systems | AM Ops Team | Run anti-virus scan on all systems | NIL |
| 15 | Determine whether IT systems are infected with virus. If the systems is infected repeat the process | AM Ops Team | Perform the entire process if the IT systems is affected by virus | NIL |
| 16 | If the systems is not infected Close/Update the service request | AM Ops Team | Close SR | NIL |
| AMCST/ Security Admin-Airtel |
| 16 | Helpdesk services/ Incident & problem management | Helpdesk |  |  |
| 17 | Seek vendor support/ possible solution | AM Ops Team |  |  |

1. **Roles & Responsibilities**

|  |  |
| --- | --- |
| **Roles** | **Responsibility** |
| AM Ops Team |           Manual update of Malware Signature, where Automatic Updates are failing. |
|           To provide the users early Malware warnings and hoaxes. |
|           Registration of all Malware prone devices with MALWARE Team. |
| Helpdesk |           Responsibilities for logging of all users Malware report tickets |
|           Follow escalation process to on-site (if necessary) to help users eradicate infections |
|           To broadcast to user community on early Malware warnings and hoaxes with advice from SPOC |
|           During Malware outbreak, constants monitoring of the problem tickets logged by users with same problem. |
|           Inform SPOC immediately upon receiving HIGH MALWARE ALERT from MSS during non-business hours. (i.e. after office hours, public holidays and weekends) |
|           Subscribe to MVPS Malware alert notification |
| AMCST/Security Admin Airtel | Central security team is the security interface for customer. Specific responsibilities include: |
|           Collate information from all locations |
|           Validate Calculation Method used |
|           Conduct Random Sample Checks |
|           Compile Reports and Share. |

1. **Malware Code Control Reports**

* Anti-Virus clients log review
* Weekly malware management dashboard
* Monthly Summary Report

1. **Performance Metrics and Benchmarks**

**6.1 Key Performance Indicator**

|  |  |  |
| --- | --- | --- |
| **KPI** | **Data Source** | **Periodicity** |
| The virus definition shall be updated on all the servers within 2 days of receipt of new virus definition | Anti virus updation failure report | As and when required |
| Anti-virus definition updates compliance review | Anti-virus compliance review report | Monthly |

**6.2 SLAs**

|  |  |  |
| --- | --- | --- |
| **Service Provided** | **SLA parameter** | **Parameter Threshold** |
| Virus definition testing and updation at distribution servers | Turnaround time to test virus definition released and deploy on distribution servers | 98% within 2 days and 100% within next 5 days from the date of release of virus definition from the vendor |
| Anti-virus definition compliance review | Perform checks on all systems to monitor implementation of latest virus definition and submit report on a monthly basis | 100% of IT systems should be updated with latest anti-virus definition within 1 week |

Annexure :

1. Contact Details :

|  |  |  |
| --- | --- | --- |
|  | **Contact Person** | **Contact details** |
| AM Ops Team contact ( Comviva) |  |  |
| Comviva Business Head  –Airtel Money ( Comviva ) | Kevin Alexander Hawkins | [kevin.hawkins@mahindracomviva.com](mailto:kevin.hawkins@mahindracomviva.com)  +254 731 406 356 |
|  |  |  |