**Document - 7**

**Operating System Controls**

|  |  |
| --- | --- |
| **Document Control Sheet** | |
| **For Airtel Money Environment only** | |
| Document Name | Operating System Access Controls |
| Document Owner | Venkatachal Hegde |
| Effective Date | xx-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](#_Toc349817661)

[2. Scope 3](#_Toc349817662)

[3. Operating System Access Standard 3](#_Toc349817663)

[4. Roles & Responsibilities 5](#_Toc349817664)

1. **Introduction**

The Operating System Access Standard document includes directives to prevent unauthorized access to operating systems.

1. **Scope**

The scope of the Operations Security Standard extends to all systems included within the Airtel Money environment.

1. **Operating System Access Standard**

The following standards represent the set of security measures to be established on all systems in order to secure Operating system access in Airtel Money environment:

* All management consoles, security consoles, administrative accesses and critical accesses shall be limited to an identified set of machines using MAC address binding or Digital certificates.
* The management sessions, critical user sessions or publicly accessible servers shall have an appropriate session timeout set.
* All information systems within Airtel Money environment shall require authentication.
* All OS access related requests related to AM environment to be approved by Security Admin-Airtel.
* The User ID shall be standardized for ease of management.
* The system shall be configured to lock a user ID after a three unsuccessful login attempts, the ID shall remain locked till cleared by the ID administrator.
* The system shall be configured to timeout the logon prompt/window if the credentials are not entered in a predefined time
* All users including normal & privileged users, administrators, third-party support staff, and management shall have a unique System Identifier (User ID) for access to the Information Systems.
* System utilities shall only be executable under the super user/administrator login.
* All unnecessary software, network protocols, bindings & services shall be removed from the system.
* The systems shall be hardened before they are moved into production.

a. IT Operations shall use the Windows/Linux security benchmark documents

b. IT Operations shall test these configuration settings in test environment before implementing them in the production

c. IT Operations shall obtain approval from Information Security Officer (ISO)/ Central Security Team and business/application head for modifications to baseline configuration

d. ISO shall periodically perform the vulnerability assessment of critical systems

* New patches, hot-fixes, patch clusters shall be tracked and implemented in a timely fashion to prevent vulnerabilities from being exploited.
* System use shall be monitored for activities like user logon/logoff date and time, usage of Super-user ID/privileged accounts & activities performed, key events, error, exception messages and security events like failed attempts at logon, password changes etc.
* Logs of security systems like firewalls, IDS, ADS servers and proxies shall be logged on a periodic basis.
* Appropriate alarm thresholds and alerts shall be established and documented for each type of event:

1. Significant system health, performance, availability and security events shall be recorded and automated alerts generated
2. Processes and tools shall be set up to carry out either real-time monitoring or automated log searches

* Password complexity shall be established for all information systems as per the organization wide password policy.
* All systems shall use a standard clock source for synchronization to maintain the validity of logs, events and evidence for legal purposes.
* All Information systems shall be audited. The User lists, groups, password policies, file-system rights, shares, mounts, accesses to system utilities, monitoring and log management and analysis shall be audited.
* These audit trails shall be maintained securely, ideally only an auditor ID shall have access to them.
* Audit trails shall be protected from alteration, damage and overwrite.

1. **Roles & Responsibilities**

|  |  |
| --- | --- |
| **Roles** | **Responsibility** |
| System Administrator | The primary responsibility for enforcing these directives lies with IT Operations Team, Information Security Officer/ Central Security Team, application development teams and applicable to all employees and third party consultants. |

Annexure :

1. Contact Details :

|  |  |  |
| --- | --- | --- |
|  | **Contact Person** | **Contact details** |
|  |  |  |
|  |  |  |
|  |  |  |