**Process Document - 8**

**Operations Security Standards**

|  |  |
| --- | --- |
| **Document Control Sheet** | |
| **For Airtel Money environment only** | |
| Document Name | Operations Security |
| 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](#_Toc349817614)

[2. Scope 3](#_Toc349817615)

[3. Operations Security Standards 3](#_Toc349817616)

[4. Roles & Responsibilities 5](#_Toc349817617)

1. **Introduction**

The Operations Security Standard document includes different standard adopted to ensure the right and secure operation of information processing facilities.

1. **Scope**

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

1. **Operations Security Standards**

Following are standards practiced for operations security:

* IT and application development functions shall ensure development, testing and production environments are separate and developers shall not have access to production environment.
* Movement of software between environments shall only be undertaken after obtaining the appropriate sign-offs from the team leads and the application development head.
* Change management procedure shall be established.
* Critical changes to production systems shall only be undertaken after the approval of the Change Advisory Board

1. The Change Advisory Board shall consist of the application development head, IT head, PMO head and shall be chaired by the Information Security Officer (ISO)/ Central Security Team.
2. The configurations and information shall be backed up before and after executing the change.

* Administrators shall not be auditors for the same systems; similarly the developers shall not administer or audit the same system.
* Remote access to the network shall be via an approved dial-in, VPN or SSL connection.
* All remote connections shall be encrypted.
* All remote connections shall be automatically disconnected after defined period of inactivity.
* All network components not in use shall be disabled or removed to prevent inadvertent access
* Simple Network Management Protocol (SNMP, RMON) and other management protocols shall be disabled, if network management is not being performed.
* All unnecessary software, network protocols, bindings & services shall be removed from the system.
* Unwanted network clients, services and protocols shall be disabled.
* Information processing systems and facilities shall be monitored for security, availability and performance. This shall include

1. Functioning of the access control mechanisms
2. HVAC units, power units, UPS systems
3. Network connectivity within the network and with service providers

* All operational processes shall be documented and the documentation shall be secured from damage.
* IT and application development teams shall use the built-in automated audit trails for all critical system components to be able to reconstruct the following events:

1. All actions taken by users with administrative privileges
2. Invalid logical access attempts
3. Use of identification and authentication mechanisms
4. Initialization of the audit logs

* Audit logging shall be configured to track the following events:

1. All Administrator activity (startups/shutdowns and related logging, errors and exceptions)
2. All System Events/Activity
3. Account Logon events (successes and failures)
4. Account management events (user or group creation, change, deletion)
5. Password activity (set, change, invalid attempts, disabled and lockouts)
6. User rights policy changes

* The logs shall not be overwritten or rolled over. They should be periodically archived to a secure location.
* Access to the Log files shall be restricted to those with an approved business need.
* Back up audit trail files to a centralized log server or media that is difficult to alter
* The retention period for logs shall be documented and shall adhere to legal and regulatory requirements for storage and retention requirements.

1. Applicable regulatory requirements for retention shall be identified
2. IT shall provide for retaining the logs as identified by above requirements

* All critical IT assets shall be identified and monitored continuously
* Monitoring the use of information processing facilities shall be documented and explicitly authorized
  1. Only identified and authorized persons shall be allowed to perform monitoring activities on information processing facilities
* The use of network analysis/monitoring tools shall be restricted to authorized personnel
* System documentation shall be stored securely in a secure environment, e.g.: Fireproof safes.
* System documentation held on public network/Intranet/File-servers, or supplied via a public network, shall be appropriately protected e.g. extra controls to be built for system documentation on publicly accessible systems.
* Passwords, pass codes, PIN shall not be kept in the documentation.

1. **Roles & Responsibilities**

|  |  |
| --- | --- |
| **Roles** | **Responsibility** |
| IT & Applications development team/System Administrator/ IT Operations Team |           Operations Security administration |