**Process Document - 15**

**Incident Management**

15.04.2013

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document Version Control** | | | | |
| **Version** | **Date** | **Prepared By** | **Reviewed By** | **Approved By** |
| 1.0 | xx-xx-xxxx |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1. Process Overview 3](#_Toc354383196)

[2. Incident Management Process Flow 6](#_Toc354383197)

[3. Roles and Responsibilities 8](#_Toc354383198)

[4. Process KPIs, Reports and Dashboards 9](#_Toc354383199)

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

An incident response and management capability is therefore necessary for detecting incidents, minimizing loss and damage, mitigating the weaknesses that were exploited, and restoring information assets in a timely manner. To that end, this document describes the procedure for incident management, particularly for reporting, response, analysis, investigation and recovery from an information security incident reported/detected in Airtel Money environment.

**Security Incident** is defined as the act of (or the threat of) occurrence of non-compliance with the security policy, procedure, or a core security requirement that may result in:

* Loss of confidentiality of information assets.
* Compromise of integrity of information assets.
* Denial of service.
* Misuse of service, systems or information assets.
* Damage to information assets

Some examples of Information Security incidents are, but not limited to:

* Attempted or successful unauthorized access, use, disclosure, modification or destruction of information
* Interference with information technology operation
* Violation of explicit or implied acceptable usage as defined in the Information Security Policy.
* Unauthorized use/disclosure of information
* Compromised user account
* Loss or theft of information assets
* Unwanted disruption or denial of service attack
* Changes to information assets without the owner's knowledge, consent, or instruction.
* Accidental miss-categorization of information that releases it inappropriately
* Copyright infringement

**Security Incident Ticket (SIT)** is a helpdesk ticket with a unique identifiable number created to identify and track security incidents. SIT will be created each time a security incident is detected or reported in the organization.

**Incident Response Team (IRT)** is a group of people responsible for responding to a security incident reported or detected in the organization. IRT is essential for a prompt and correct response to an information security incident so it can be contained, investigated and recovered from in a timely manner thereby reducing loss to the organization.

**Entry Criteria**

* Information Security Incident is reported
* Information Security Incident is detected

**User Responsibility**

* It is the responsibility of each employee and third party user to report any observed or suspected deviations from the organization’s information security policies, procedures and associated documents, and/or weaknesses to IT helpdesk team as information security incident.
* Employees and third party users shall not attempt to prove any suspected security weakness. Testing weaknesses could cause damage to the information system or service; it would be interpreted as a potential misuse of information system and may result in disciplinary action for the individual performing the testing.

**IT Helpdesk Responsibility**

IT helpdesk team shall:

* Notify IRT in a timely manner of any incident detected/reported that require immediate attention.
* Ensure that personnel dealing with the information security incidents reported/detected are within the team to deal with an information security incident
* Record incident details in preliminary incident report
* Work closely with incident response team to ensure availability of IT Infrastructure as required during the course of incident response, investigation or recovery
* Wherever required, work with IRT to arrange support of Product Vendors
* Ensure that data and information found during investigation is not tampered with deliberately or unknowingly by IT personnel during maintenance or other activities
* Notify and update the user of status of SIT logged by him/her.

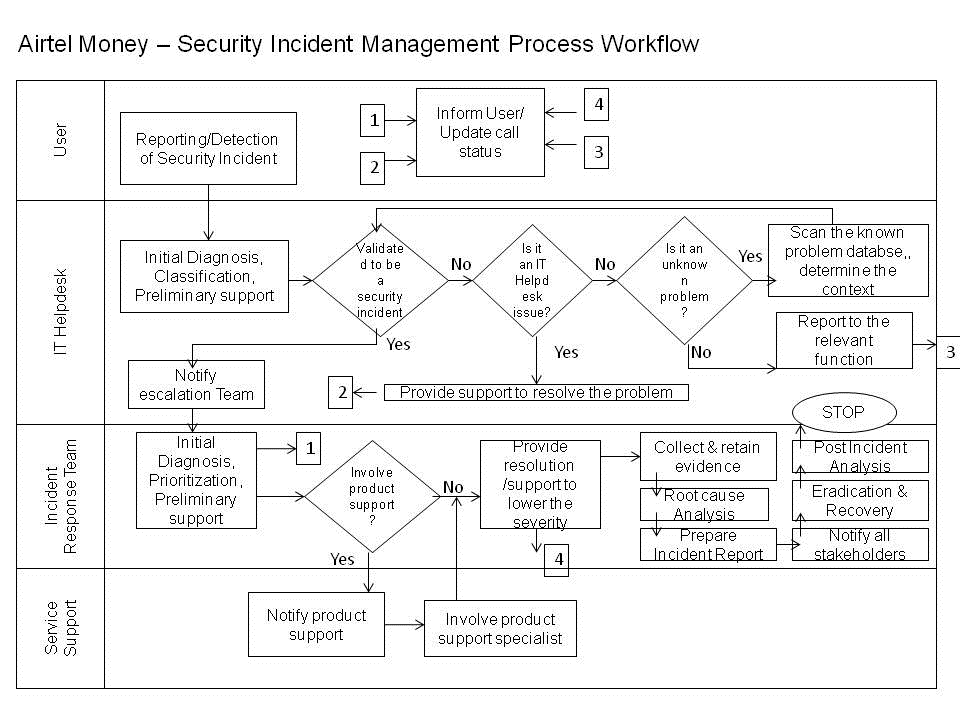
**Incident Response Team**

Incident Response Team (IRT) consists of representation from the following functions within the organization to respond and manage information security incidents, and other unanticipated situations that may transform into an incident:

* Information Technology and Innovation: For all issues and incidents related to IT infrastructure and non-compliance with the organization’s information security policies.
* Human Resources and Administration:
  + Human Resources: For assistance with disciplinary proceedings or employee counselling when an employee is the apparent target of an incident or is suspected of causing an incident.
  + Administration: To ensure coordination between physical security and IRT, and respond to reported physical infrastructure security incidents.
* Legal and Regulatory:
* For reviewing incident response policies and procedures to ensure their compliance with applicable law and regulatory requirements.
* For guidance wherever incident may have legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit.
* Finance and Business Integration: For understanding financial implications and penalties associated with information security incidents.
* Marketing and Communication: For response to media and public within the constraints imposed by security and law enforcement interests.
* Networks: For all issues and incidents related to telecom infrastructure and networks.

.

1. **Incident Management Process Flow**



**Incident Management Process Work Flow**

**Reporting / Detection of Information Security Incident**

* The user reports a potential information security incident *via* intranet module, electronic mail (e-mail), telephone or in person to IT helpdesk team. For every information security incident reported, a security incident ticket is generated and assigned for action to the IT helpdesk team.
* Where potential information security incident is detected during routine operational and/or monitoring activities, a security incident ticket will be generated, and assigned for action to the IT helpdesk team.

**Initial Diagnosis, Classification and Preliminary Support – IT helpdesk Team**

* IT helpdesk team performs initial diagnosis and, if required, provides immediate support to contain the incident. Wherever possible and required, IT helpdesk team will prepare a preliminary incident report with the following information:
* Description of Incident
* Possible Causes
* Damages Observed
* Supporting Evidence
* Remedial Steps Taken

This preliminary investigation report will be forwarded to IRT at the time of notification of the incident.

* IT helpdesk team will notify the IRT if the incident qualifies as an information security incident.
* If not, IT helpdesk team determines if the incident is an IT Issue that can be addressed within the team.
* If the issue is neither an information security incident nor an IT Helpdesk issue, IT helpdesk team will scan the ‘known problem’ database (knowledgebase, known bug lists, planned outage reports, communication from vendor, vulnerability database and similar repositories) to determine the problem context and a likely resolution.
* Based on the problem context, IT helpdesk team will then inform the relevant department/function of the problem, and notify the user of the same.
* In case of a non-IT related problem, IT helpdesk team will inform the relevant department and notify the user of the status

**Incident Handling - IRT**

* On receiving notification about the incident from IT helpdesk team, IRT will perform initial diagnosis and provide preliminary support, if required to contain the incident. In addition, IRT will classify the incident based on Incident Priority Matrix.
* IRT will also send out an incident alert to users and relevant departments who could be possibly affected by the incident. The incident alert will contain incident symptoms and actions to be taken by the user.
* If the incident involves a proprietary software or hardware, IRT (if required in coordination with IT helpdesk team) will contact the product vendor for support and work jointly to resolve the issue.
* IRT will then work towards providing resolution and support to resolve the incident.
* IRT shall collect and maintain relevant evidence, associated with the incident as per Electronic Evidence Management Guideline.
* IRT will work to conduct a root cause analysis and prepare a report of the incident based on the information collected by the concerned IRT member and the preliminary report submitted by IT helpdesk team.A detailed incident report shall be submitted within 3 days of the incident. IRT shall additionally perform forensic analysis on each IT-related, high and medium level incidence.
* Once the incident has been analyzed and evidence has been collected, IRT will notify the stakeholders within the organization. In a case where notification of incident is vital for the continuity of business, IRT will inform the stakeholders at any time during incident-handling.
* Once the incident has been resolved or contained, eradication of incident components will be done by IRT (solely or jointly with relevant stakeholder(s) for e.g., product/service vendor or application developer) to contain the incident
* IRT will suggest through appropriate communication mechanisms (such as system notifications, e-mails or oral warnings) to the relevant stakeholders, methodologies for recovering from the incident. Such methodologies will include restoring systems to their normal operations, cleaning up of residual incident components and suggestions for strengthening the systems.
* As part of post-incident analysis and activities, IRT will analyze incident reports and determine corrective and preventive actions to limit similar incidents in future.

1. **Roles and Responsibilities**

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

* 1. **Incident manager**

The Incident manager is responsible for:

* Drive the efficiency and effectiveness of Incident Management process.
* Coordinate the work of incident support staff and support levels involved in Incident Management.
* Coordinate with Problem Management for workarounds and solutions
* Conduct Trend Analysis of incldents and service requests and refer potential problems to problem management
* Ensure adequate support for Manor incidents and should maintain a list of who should be contacted during Major Incidents.
* Provide Management Information and process reports
* Review Incident management process and identify improvement opportunities through Process Improvement Plans
* Ensure clear, complete and periodic communication throughout the major incident lifecycle
  1. **IT Helpdesk Team**
* Incident Registration
* Routing service requests to support groups wherever necessary
* Initial support and classification
* Resolution and recovery of minor incidents
* Communication to the user on the status throughout the incident lifecycle
* Informing the user/customers of possibility of SLA breaches in case the resolution is getting delayed.
  1. **Service support ( L1/L2/L3 )**
* Handling service requests
* Monitoring Incident details, including the Configuration Items affected
* Incident investigation and Diagnosis ( including resolution where possible)
* Detection of possible problems and coordination with problem management
* The resolution and recovery of assigned incidents

1. **Process KPIs, Reports and Dashboards**

The Incident Manager needs to provide ongoing reporting around the KPIs and process related metrics and trends that indicate the health of the process 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 Performance Indicators ( KPIs) :

1. Number of escalations includes (# of incidents not resolved in the agreed resolution time.
2. Incident Resolution Time : Average time for resolving an incident ( per category) Frequency daily
3. Resolution within SLA – Rate of incidents resolved during solution times agreed in SLA ( per category)
4. Status of Open Tickets. with ageing.
5. Incident Management process Audit Report : Daily audit report on process compliance
6. Daily Report on Open Global Incidents if any
7. Weekly Status report on open L3 tickets.

Annexure :

1. Contact Details :

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