## INCIDENT MANAGEMENT PROCESS

<table>
<thead>
<tr>
<th>Code:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version:</td>
<td></td>
</tr>
<tr>
<td>Date of version:</td>
<td></td>
</tr>
<tr>
<td>Created by:</td>
<td></td>
</tr>
<tr>
<td>Approved by:</td>
<td></td>
</tr>
<tr>
<td>Confidentiality level:</td>
<td></td>
</tr>
</tbody>
</table>

**Comment [BV1]:** All fields in this document marked by square brackets [ ] must be filled in.


**Comment [BV3]:** The document coding system should be in line with the organization’s existing system for document coding; in case such a system is not in place, this line may be deleted.
Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Created by</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>xx/xx/2013</td>
<td>0.1</td>
<td>Branimir Valentic</td>
<td>Basic document outline</td>
</tr>
</tbody>
</table>

Table of contents

1. PURPOSE, SCOPE AND USERS........................................................................................................3
2. REFERENCE DOCUMENTS .............................................................................................................3
3. PROCESS ACTIVITIES ...................................................................................................................4
   3.1. INCIDENT IDENTIFICATION.................................................................................................5
   3.2. INCIDENT LOGGING ............................................................................................................5
   3.3. INCIDENT CATEGORIZATION ............................................................................................6
   3.4. INCIDENT PRIORITIZATION...............................................................................................6
   3.5. INITIAL DIAGNOSIS .........................................................................................................7
   3.6. ESCALATION ....................................................................................................................7
   3.7. INVESTIGATION AND DIAGNOSIS ....................................................................................8
   3.8. RESOLUTION AND RECOVERY .........................................................................................8
   3.9. INCIDENT CLOSURE .........................................................................................................8
   3.10. REOPENING ...................................................................................................................8
   3.11. MAJOR INCIDENT ...........................................................................................................8
4. ROLES AND RESPONSIBILITIES....................................................................................................9
   4.1. INCIDENT MANAGER .......................................................................................................9
   4.2. FIRST-LINE ANALYST (1ST LEVEL) ................................................................................9
   4.3. SECOND-LINE ANALYST (2ND LEVEL) ............................................................................9
   4.4. SERVICE Desk .................................................................................................................9
5. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT...........................................10
6. VALIDITY AND DOCUMENT MANAGEMENT .......................................................................10
7. APPENDICES............................................................................................................................10

©2013 This template may be used by clients of EPPS Services Ltd. www.20000academy.com in accordance with the License Agreement.
1. Purpose, scope and users

The aim of this document is to define the purpose, scope, principles and activities for the Incident Management process.

This document is applied to the entire IT organization.

Users of this document are all employees of [organization name], as well as all external parties who have a role in IT Service Management (ITSM).

2. Reference documents

- Incident Management Policy
- Incident Measurement and Metrics
- Problem Management Process
- Release and Deployment Management Process
- Service Asset and Configuration Management Process
- Service Level Agreement Management Process
- Information Security Management Process
Figure: Incident Management process activities

Incidents can be detected by several means: Incident staff, users, event monitoring tools and their actions, e.g. notifications.

3.1. Incident identification

This is the stage where an Incident has been recognized. Sources of an Incident are:

<table>
<thead>
<tr>
<th>Source</th>
<th>Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web portal: [insert web or intranet address]</td>
<td>User</td>
</tr>
<tr>
<td>Phone:</td>
<td>Service Desk staff</td>
</tr>
<tr>
<td>☐ During agreed service hours: [insert phone number in appropriate format]</td>
<td></td>
</tr>
<tr>
<td>☐ Outside agreed service hours: [...]</td>
<td></td>
</tr>
<tr>
<td>E-mail [...].</td>
<td>Event Manager</td>
</tr>
</tbody>
</table>

[Service Desk staff] is responsible to pass Request Fulfillment process by [...].

3.2. Incident logging

An incident can be logged by:

a) User
   - Using web portal, [insert web or intranet address]
   - E-mail [...]
   - Phone:
     - ☐ During agreed service hours: [insert phone number in appropriate format]
     - ☐ Outside agreed service hours: [...]  

b) Event tool: [enter tool(s) name]

Organization uses [tool name] tool for Incident Management.

Service Desk staff is responsible for entering incident data.

Mandatory data that need to be recorded are:

- Incident number – provided automatically
- Incident title / description
- User name / department / location (if other than Requestor)
- Requestor, date and time
- Incident category
- Description

Incident assignees are responsible, as the incident progress to the resolution, for ensuring that every resolution is available.
3.3. **Incident categorization**

During the logging phase, incidents are categorized. Service Desk staff categorizes incidents by phase. Categories of incidents opened by other assets are verified by the Service Desk and can be re-categorized.

Categories are set in 3 levels as defined in the Incident Catalogue; see Incident Catalogue in Appendix.

3.4. **Incident prioritization**

[role description] is responsible for ensuring that every incident is prioritized. Priority consists of impact and urgency based on the following table:

<table>
<thead>
<tr>
<th>Impact</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

Resolution time of an incident depends on its priority code and is calculated as follows:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Description</th>
<th>Target Resolution Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Critical</td>
<td>Graded</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Planned</td>
<td>24 hours</td>
</tr>
</tbody>
</table>

Impact – business impact causes:

<table>
<thead>
<tr>
<th>Impact</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>30% - 50% of users are affected</td>
<td>Less than 30% of users are affected</td>
</tr>
<tr>
<td>Medium</td>
<td>10% - 20% of users, 5% - 10% of services are affected</td>
<td>Less than 35% of services are affected</td>
</tr>
<tr>
<td>Low</td>
<td>1% - 5% of users, 1% - 5% of services are affected</td>
<td></td>
</tr>
</tbody>
</table>

Urgency – how quickly the business needs a resolution:

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>_available workaround exists</td>
<td>in the long term a good workaround exists</td>
</tr>
<tr>
<td>Medium</td>
<td>available</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>available</td>
<td></td>
</tr>
</tbody>
</table>
Change of priority – the priority is defined by a user and can be changed by the Service Desk or incident assignee.

VIP treatment – priority for VIPs is [...].

3.5. Initial diagnosis

Initial diagnosis is performed by [role description], with the goal being to resolve the incident without investigation or, if that is not possible, to collect as much relevant information as possible for further diagnosis.

Matching of incidents to problems and known errors during initial diagnosis aims to resolve incidents as quickly as possible and/or save time needed for escalation.

To use existing information and knowledge, [incident assignee] has access to and uses the following resources:

- Known Errors – see Known Error in Appendix of Problem Management Process
- Problem Record in Appendix of Problem Management Process
- Configuration Management Database (CMDB) – see CMDB in Appendix of the Service Asset and Configuration Management Process
- Release report and Release plan – see Release and Deployment Planning in Appendix of the Release and Deployment Management Process

3.6. Escalation

There are two escalation possibilities:

- Functional escalation
- Hierarchical escalation

The Service Desk is responsible for the resolution of the incident during the escalation procedure. This includes tracking progress, keeping users informed and incident closure.

3.6.1. Functional Escalation

Functional escalation is triggered by [role description]/[tool name]. Functional escalation of an incident is escalation to specialist group. The OLA (Operation Level Agreement) and UC (Underpinning Contract) define under which circumstances an incident will be escalated. The Service Desk is responsible for escalation if more than one support group is involved in incident resolution.

3.6.2. Hierarchical Escalation

Hierarchical escalation is triggered by [role description]/[tool name]. Hierarchical Escalation is used in the following situations:

- For high priority incidents – Service Level Manager is informed about such incident
- When resolution of an incident reaches beyond [target resolution time]

When it is triggered by a user or customer management [role description] is responsible to handle such escalation and inform [role description].
[role description] ensures that Investigation and diagnosis of an incident is in agreed Resolution Time (see Service Level Agreement in Appendix of Service Level Management Process). [role description] is responsible for coordination of all activities, particularly those which involve
more than one support group.

3.7. Investigation and diagnosis

[role description] ensures that investigation and diagnosis of an incident is completed within the agreed Resolution Time (see Service Level Agreement in Appendix of Service Level Management Process). [role description] is responsible for coordination of all activities, particularly those which involve more than one support group.

3.8. Resolution and recovery

[role description] is responsible for the following:
- To define personnel responsible for resolution test and application
- To ensure
- To coordinate activities
- When successfully resolved, the resolving group passes the incident back to Service Desk for closure action.

3.9. Incident closure

The Service Desk checks that the customer is willing to agree that the incident can be closed.

When a resolution is implemented, the Service Desk changes the incident’s status to “Resolved.” The incident is then moved to the “Closed” stage automatically.

3.10. Reopening

Incidents are reopened in the Incident Policy.

3.11. Major incident

Major incidents are incidents with higher impact, resulting in significant disruption of services, and need special attention to resolve them. Major incidents, as defined in Service Level Management (see Service Level Agreement in Appendix of Service Level Management), [role description] is responsible for:
- Reporting to the [top management]
- Definition of major incident procedure (as part of SLA) that should define:
  - Declaration of major incident
  - Management, i.e. handling of major incidents
  - When and where to communicate during and following major incidents

Comment [BV51]: List all interested parties.
Comment [BV52]: Service Level Manager role on customer side.
Comment [BV53]: Adapt to your own requirements. This should be defined in SLA.
Comment [BV54]: ***OPTION*** Delete this section if you are implementing ITIL and not ISO 20000.
Comment [BV55]: DELETE what is unnecessary.
Comment [BV56]: Insert role. Usually this is done by Incident Manager.
Comment [BV57]: If you want to learn more about incident resolution and closure, see http://www.20000academy.com/2013/Incident-resolution-and-closure-waiting-for-the-fat-lady-to-sing/.
Comment [BV58]: Insert role. Usually this is done by Incident Manager.
Comment [BV59]: Change if needed. Example: Incident Manager, Resolving Group Manager, etc.
Comment [BV60]: Service Desk is responsible for the whole lifecycle of an Incident. If no Service Desk in place – define role which will close the incident.
Comment [BV61]: Service Desk is responsible for the whole lifecycle of an Incident. If no Service Desk in place – define role which will perform this action.
Comment [BV62]: Delete redundant.
Comment [BV63]: Delete this paragraph.

This can be done for all incidents or just for some of them, e.g. VIP incidents or Major incidents.

Comment [BV64]: ***OPTION*** Delete this section if you are implementing ISO 20000 and not ITIL.
Comment [BV65]: Insert role.
Comment [BV66]: Adapt to your own conditions in SLA.
Comment [BV67]: This is, usually, Incident Manager.
Comment [BV68]: Insert correct function of top management. Example: Support group, Service Desk.
Comment [BV69]: A clear trigger must
Comment [BV70]: To whom? E.g. Support group, Service Desk.
4. Roles and responsibilities

4.1. Incident Manager

[role description] assigns the Incident Manager role.

Responsibilities of Incident Manager:
- Overall responsibility for carrying out activities within the scope of Incident Management
- Coordinates with other Service Management roles
- Plans and/or participates in support Incident Management process
- Responsible for reporting and managing information
- Manages work of incident staff
- Monitors and maintains incident management process and procedures
- Manages of incidents throughout first-, second- and third-line analysts

4.2. First-Line Analyst (1st Level)

[role description] assigns the First-Line Analyst role.

Responsibilities of First-Line Analyst:
- Incident recording
- Incident classification, prioritization and escalation
- Resolution and recovery of incidents
- Monitoring the status and progress of assigned incidents
- Closing of incidents
- Informing users and Service Desk about incident progress
- Updating Incident Record

4.3. Second-Line Analyst (2nd Level)

[role description] assigns the Second-Line Analyst role.

Responsibilities of Second-Line Analyst:
- Same as First-Line Analyst, but with
  - Deeper technical knowledge and time direction to incident resolution.

4.4. Service Desk

Service Desk is a function, and is defined in the document “Service Desk Function.”
5. Managing records kept on the basis of this document

<table>
<thead>
<tr>
<th>Record name</th>
<th>Storage location</th>
<th>Person responsible for storage</th>
<th>Controls for record protection</th>
<th>Retention time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Record (in electronic form)</td>
<td>[tool name]</td>
<td>[role description]</td>
<td>Service Desk, 1st Level and 2nd Level have right to add to /change the record.</td>
<td>Incident Records are kept for [...].</td>
</tr>
<tr>
<td>Reports</td>
<td>[tool name]</td>
<td>[role description]</td>
<td>Incident Manager</td>
<td>Reports are kept for [...].</td>
</tr>
<tr>
<td>Customer Satisfaction Survey</td>
<td>[Service Knowledge Management System – SKMS]</td>
<td>[role description]</td>
<td>Incident Manager</td>
<td>Reports are kept for [...].</td>
</tr>
<tr>
<td>Reopened Incidents</td>
<td>[tool name]</td>
<td>[role description]</td>
<td>Reopening of Incident Record can be done only by [role description].</td>
<td>Reports are kept for [...].</td>
</tr>
</tbody>
</table>

6. Validity and document management

This document is valid as of [date].

Owner of this document is [role description], who must document at least once a year.

7. Appendices

- Appendix 1: Incident Catalogue
- Appendix 2: Incident Record
- Appendix 3: Major Incident Report
Comment [BV88]: Only necessary if the Procedure for Document Control prescribes that paper documents must be signed.
Insert correct function of top management. Example: IT manager, Board of Management, CEO, Company President...etc.

A clear trigger must be defined,