# INCIDENT MANAGEMENT POLICY

<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 [BV2]: 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.

Comment [BV1]: All fields in this document marked by square brackets () must be filled in.
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 template</td>
</tr>
</tbody>
</table>

Table of contents

1. PURPOSE, SCOPE AND USERS ................................................................. 3
2. REFERENCE DOCUMENTS ........................................................................... 3
3. POLICY ........................................................................................................ 3
   3.1. INCIDENT MANAGEMENT ................................................................. 3
   3.2. COMMUNICATION ............................................................................. 3
   3.3. TIMEFRAME ...................................................................................... 4
   3.4. CUSTOMER SATISFACTION ................................................................. 4
   3.5. REOPENING OF INCIDENTS ............................................................... 4
   3.6. INCIDENT RECORDS .......................................................................... 4
   3.7. MEASUREMENT .................................................................................. 5
4. VALIDITY AND DOCUMENT MANAGEMENT .................................................. 5
1. **Purpose, scope and users**

The purpose of this policy is to ensure that any incidents that affect the daily operations of [organization name] are managed through an established process.

This policy applies to all [company name] full-time, part-time and contracted employees, vendors and suppliers involved in activities that use or manage technology solutions within [company name].

Users of this document are employees of [IT service management organization].

2. **Reference documents**

   - Incident Management Process
   - Service Level Management Process
   - Measurement and Metrics
   - Business Relationship Management Process
   - Information Security Management Process
   - Communication Procedure

3. **Policy**

   3.1. **Incident Management**

   The purpose of the Incident Management process is to restore IT service as quickly as possible, minimize impact on business operation and ensure that agreed service levels are kept [see Incident Management Process].

   **All incidents of [organization name] are managed according to the Incident Management process.**

   The scope of the Incident Management process encompasses all incidents from operational services (see Service Portfolio in Appendix of Service Portfolio Management Process) as well as information security incidents (see Information Security Management Process).

   The goal of Incident Management is to:
   - increase customer satisfaction with provided services through efficient incident management
   - introduce and manage standardized process for resolving incidents
   - introduce, maintain and improve communication between ITSM organisation and users and customers

   3.2. **Communication**
[role description] is responsible to define communication methods and responsibilities between different support groups, as well as toward Service Desk and users. Users are persons who use the service on a daily basis. Hereafter, they are referred to as “users.”

In order to ensure that information is shared in a timely manner (when needed, throughout the process), the right and appropriate channels are used to reach the level of parties involved and with whom needed (both internally toward IT or externally toward users), [role description] is responsible to:

- Educate Service Desk staff, 1st Level, 2nd Level – see Incident Management Process
- Introduce technological solutions:
  - E-mail
  - [tool name]
  - Telephone
  - [...]

[role description] is responsible to inform the customer about the progress and the resolution of incidents they opened.

The Communication Procedure is defined in the document “Communication Procedure.”

3.3. Timeframe

The timeframe in which incidents must be resolved are defined in the Service Level Agreement (SLA), Underpinning Contract (UC) and Operational level Agreement (OLA) according to the Service Level Management process. [role description] is responsible for definition of timeframe and implementation in [tool name] tool.

3.4. Customer Satisfaction

Customer satisfaction is measured in the following way:

a) After an incident is resolved, the user can send feedback via a resolved incident ticket three days after Incident achieves Resolved status. [role description] creates a report showing the measures taken and findings for [role description].

b) Satisfaction Survey in Appendix of Business Relation Management Process. Findings of the survey will be reported to [role description].

3.5. Reopening of Incidents

Incidents can be reopened by [role description]. Reopening of Incidents can occur, at the latest, two days after the incident was resolved. Reopened Incidents, with reasoning, must be reported to [role description] on a monthly basis, using [...].

3.6. Incident Records

All incident records are kept and managed in a single management system. [tool name] is used for that purpose. All employees of [name of the IT Service Management Department] are obliged to enter and update all statuses and detailed data.
[role description] is responsible to audit incident records' integrity [once a year].

The audit includes checking of the following parameters:
- All status updates are entered
- Incidents are correctly classified
- Incidents are correctly prioritized

3.7. Measurement

Measurement and metrics requirements are defined in the document "Measurement and Metrics."

4. Validity and document management

This document is valid as of [date].

Owner of this document is [job title], who must [check and, if necessary, update the document at least once a year].

[job title]

[name]

[signature]

Comment [BV22]: Enter responsible person: This should be someone who is independent from IT Service Management organization (e.g. someone from Quality Management).

Comment [BV23]: Change if necessary.

Comment [BV24]:

Comment [BV25]: This is only a recommendation; adjust frequency as appropriate.

Comment [BV26]: Only necessary if the Procedure for Document Control prescribes that paper documents must be signed.