

**INCIDENT MANAGEMENT POLICY**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc384289491)

[2. Reference documents 3](#_Toc384289492)

[3. Policy 3](#_Toc384289493)

[3.1. Incident Management 3](#_Toc384289494)

[3.2. Communication 3](#_Toc384289495)

[3.3. Timeframe 4](#_Toc384289496)

[3.4. Customer Satisfaction 4](#_Toc384289497)

[3.5. Reopening of Incidents 4](#_Toc384289498)

[3.6. Incident Records 4](#_Toc384289499)

[3.7. Measurement 5](#_Toc384289500)

[4. Validity and document management 5](#_Toc384289501)

# 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].

# Reference documents

* Incident Management Process
* Service Level Management Process
* Measurement and Metrics
* Business Relationship Management Process
* Information Security Management Process
* ISO/IEC 20000-1:2011, clause 8.1.
* Communication Procedure
* ISO/IEC 20000-1:2011, clause 6.6.3.
* ISO 27035 varies clauses

# Policy

## 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-related 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 organization and users and customers

## 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 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 complete incident lifecycle), in the right wording (appropriate respective to 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 of the resolution of incidents they opened.

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

## 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.

## Customer Satisfaction

Customer satisfaction is measured in the following way:

1. After an Incident is resolved, the user can send feedback via a resolved Incident ticket three business days after Incident achieves Resolved status. [role description] creates a report based on user feedback on a monthly basis and reports findings to [role description].
2. Once a year, [role description] will perform a Customer Satisfaction Survey; see Customer Satisfaction Survey in Appendix of Business Relation Management Process. Findings of the survey will be reported to [role description].

## 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 by [role description] to [role description] on a monthly basis, using […].

## 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

## Measurement

Measurement and metrics requirements are defined in the document “Measurement and Metrics.”

# 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.