[Organization logo]

[Organization name]

INCIDENT MANAGEMENT PROCESS

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

Commented [20A1]: All fields in this document marked by square brackets [ ] must be filled in.

Commented [20A2]: If you want to find out more about Incident Management, see https://advisera.com/20000academy/blog/2013/05/21/incident-management-itil-solid-foundations-operational-processes/

Commented [20A3]: 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

Date	Version	Created by	Description of change
	0.1	20000Academy	Basic document outline

Table of contents

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 all processes and activities in the SMS.

Users of this document are all employees of [organization name], as well as all external parties who have a role in the SMS.

Commented [20A4]: Please include the name of your company.

2. Reference documents

- ISO/IEC 20000-1:2018, clauses 7.5.4.e), 8.6.1.
- Change Management Process
- Problem Management Process
- Configuration Management Process
- Release and Deployment Management Process
- Information Security Management Process
- Service Level Management Process

Commented [20A5]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder “09_Service_Design_Build_Transition_Processes/ 09.1_Change_Management”.

Commented [20A6]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder “10_Resolution_Fulfilment_Processes/ 10.3_Problem_Management”.

Commented [20A7]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder “06_Service_Portfolio_Processes/ 06.3_Configuration_Management”.

Commented [20A8]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder “09_Service_Design_Build_Transition_Processes/ 09.3_Release_and_Deployment_Management”.

Commented [20A9]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder “11_Service_Assurance_Processes/ 11.3_Information_Security_Management”.

Commented [20A10]: You can find a template for these documents in the ISO 20000 Documentation Toolkit folder “07_Relationship_Agreement_Processes/ 07.2_Service_Level_Management”.

3. Process overview

The purpose of the Incident Management process is to [illegible]

The scope of the Incident Management process encompasses all incidents from operational services [illegible]

Commented [20A11]: [illegible]

The objectives of the Incident Management process are as follows:

- increase customer satisfaction with provided services through efficient incident management
- [illegible]
- [illegible]

Commented [20A12]: These are recommended objectives; you can include additional objectives or delete some according to your company practices.

4. Process activities

The incident assignee is responsible for ensuring, [illegible]

Commented [20A13]: [illegible]

4.1. Incident recording

[illegible]

Incidents can be recorded by:

a) User
   - [illegible]
   - [illegible]
   - [illegible]
     - [illegible]
     - [illegible]

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

[illegible]

Mandatory data that need to be recorded are:

- Incident number – provided automatically
- Requestor name / department / location
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

4.2. Incident prioritization

The First-Line Analyst is responsible for ensuring that every incident is prioritized. Priority consists of impact and urgency, [illegible]

[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

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

Priority code	Description	[illegible]
1	Critical	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

Impact – business impact that an incident causes:

High	Medium	Low

Commented [20A14]: [illegible]

Commented [20A15]: [illegible]

Commented [20A16]: [illegible]

Commented [20A17]: [illegible]

Commented [20A18]: [illegible]

Commented [20A19]: [illegible]

Commented [20A20]: [illegible]

Commented [20A21]: You can adapt this according to your company practices.

Commented [20A22]: Choose the one that applies.

Commented [20A23]: [illegible]

Commented [20A24]: Delete if not true.

Commented [20A25]: These are data that are always needed and cannot be deleted.

[illegible]

Commented [20A26]: This is only a recommendation; you can adapt the priority levels according to your company practices.

Commented [20A27]: Should be adapted according to: [illegible]

[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

Urgency – how quickly the business needs a resolution:

High	Medium	Low
[illegible]	[illegible]	[illegible]

Change of priority – priority defined by a user [illegible]

4.3. Incident classification

After prioritization, incidents are classified. [illegible]

Incidents will be assigned one of the following classifications:

- Software
    - Office automation
    - Internet Explorer
    - Word
    - Excel
- [illegible]
    - [illegible]
    - [illegible]
- [illegible]
    - [illegible]
    - [illegible]
    - [illegible]
    - [illegible]
- [illegible]
    - [illegible]
    - [illegible]
    - [illegible]
- [illegible]

Information security incidents are classified as [Information Security] and priority is established using [illegible]

Commented [20A28]: [illegible]

Commented [20A29]: [illegible]

Commented [20A30]: [illegible]

Commented [20A31]: Choose the one that applies according to your company practices.

Commented [20A32]: [illegible]

Commented [20A33]: [illegible]

Commented [20A34]: [illegible]

Commented [20A35]: [illegible]

Commented [20A36]: This is just an example. Edit or add new entries according to your company practices.

Commented [20A37]: Please adjust this according to your company practices.

This should correspond to the incident classification field in the Incident Record.

Commented [20A38]: [illegible]

The Change Manager is responsible to decide which changes will be handled through the Incident Management process.

4.4. Escalation

In order to resolve the incidents as quickly as possible and/or save time needed for escalation, [illegible] resources:

- Known Errors
- [illegible]
- [illegible]
- [illegible]

If incidents cannot be resolved, the escalation procedure is carried out. There are two escalation possibilities:

- [illegible]
- [illegible]

[illegible] keeping customers informed of their reported incident, and closure.

4.4.1. *Functional Escalation*

Functional escalation is triggered by [job title] / [tool name] tool. Functional escalation of an incident is escalation to a specialist group. [illegible]

4.4.2. *Hierarchical Escalation*

[illegible]

- [illegible]
- [illegible]
- [illegible]

The employee who performs the escalation is responsible to handle such escalation and inform the Incident Manager.

If so agreed in the SLA, the Incident Manager informs the Service Level Manager [illegible]

4.5. Resolution

Commented [20A39]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder “10_Resolution_Fulfilment_Processes/ 10.3_Problem_Management”.

Commented [20A40]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder “10_Resolution_Fulfilment_Processes/ 10.3_Problem_Management”.

Commented [20A41]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder “06_Service_Portfolio_Processes/ 06.3_Configuration_Management”.

Commented [20A42]: You can find a template for this document in the ISO 20000 Documentation Toolkit folder “09_Service_Design_Build_Transition_Processes/ 09.3_Release_and_Deployment_Management”.

Commented [20A43]: These are only examples; you can delete some or include additional resources according to your company practices.

Commented [20A44]: Change if needed.

Commented [20A45]: Please insert the appropriate job title according to your organization practices, e.g.: Incident Manager, 1st Line Analyst, etc.

Commented [20A46]: [illegible]

Commented [20A47]: Change if needed

Commented [20A48]: [illegible]

Commented [20A49]: [illegible]

Commented [20A50]: [illegible]

The Incident Manager ensures that resolution of an incident remains within the agreed resolution time as defined in the Service Level Agreement. [illegible]

The Incident Manager is responsible for the following:

- To define personnel responsible for resolution test and application
- [illegible]
- [illegible]

[illegible]

[illegible]

When a resolution is implemented, the First-Line Analyst changes the status to “Resolved.” The user [illegible]

If incidents are classified as information security incidents, after the incidents are resolved, the Information Security Manager is responsible to:

- [illegible]
- [illegible]
- [illegible]

4.6. Major incident

Major incidents are incidents with higher impact, resulting in significant disruption of the services, and need special attention to resolve them. Major incidents are customer-specific, are defined on a customer basis, and are a mandatory part of the SLA. The Incident Manager is responsible for:

- Reporting to the [job title]
- [illegible]
    - [illegible]
    - [illegible]
    - [illegible]
    - [illegible]
    - [illegible]

The Business Relationship Manager is responsible to communicate progress, activities, and results to the customer as they are documented in the Major Incident Report.

5. Roles and responsibilities

5.1. Incident Manager

Commented [20A51]: You can find a template for these documents in the ISO 20000 Documentation Toolkit folder “07_Relationship_Agreement_Processes/ 07.2_Service_Level_Management”.

Commented [20A52]: These are only examples; you can delete some or include additional elements according to your company practices.

Commented [20A53]: [illegible]

Commented [20A54]: [illegible]

Commented [20A55]: Choose the one that is applicable according to your company practices.

Commented [20A56]: [illegible]

Commented [20A57]: These are mandatory, so please don’t delete them. You may include additional elements according to your company practices.

Commented [20A58]: Please insert the appropriate job title from the top management according to your organization practices, e.g.: CEO, CIO, IT Director, IT Manager, etc.

Commented [20A59]: [illegible]

Commented [20A60]: [illegible]

Commented [20A61]: These are mandatory, so please don’t delete them. You may include additional elements according to your company practices.

[Job title] assigns the Incident Manager role.

Responsibilities of Incident Manager are:

- Overall responsibility for carrying out activities within the scope of Incident Management
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

[illegible]

Responsibilities of First-Line Analyst:

- Incident recording
- Incident classification, prioritization and escalation
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

5.3. Second-Line Analyst (2nd Level)

[Job title] assigns the Second-Line Analyst role.

Responsibilities of Second-Line Analyst:

- [illegible]

6. Measurement and reporting

The Incident Manager is responsible to:

- Define and review [illegible] objectives defined in the SMS Plan and corresponding Key Performance Indicators (KPIs) that can be used to monitor the progress on the achievement of the CSFs
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Commented [20A62]: Please insert the appropriate job title according to your organization practices, e.g.: IT Manager, Service Manager, etc.

Commented [20A63]: These are only examples; you can delete some or include additional elements according to your company practices.

Commented [20A64]: [illegible]

Commented [20A65]: [illegible]

Commented [20A66]: These are only examples; you can delete some or include additional elements according to your company practices.

Commented [20A67]: [illegible]

Commented [20A68]: [illegible]

Commented [20A69]: [illegible]

Commented [20A70]: You can find a template for this document in the ISO 20000 Toolkit folder "13_Management_Review".

Commented [20A71]: [illegible]

Commented [20A72]: [illegible]

Commented [20A73]: You can change the frequency according to your company practices.

- [redacted]

[redacted] in the Matrix of Process Measurements to reflect the new objectives.

Commented [20A74]: You can find a template for this document in the ISO 20000 Toolkit folder “13_Management_Review”.

7. Managing records kept on the basis of this document

Record name	*Storage location*	*Person responsible for storage*	*Controls for record protection*	*Retention time*
Incident Record (in electronic form)	[tool name]	Incident Manager	First-Line Analyst and Second-Line Analyst have the right to add/change the record.	Incident Records are kept forever.
Major Incident Report	[tool name]	Incident Manager	Incident Manager	Major Incident Reports are kept forever.
Reports	[tool name]	Incident Manager	Incident Manager	Reports are kept for [3 years].

Commented [20A75]: Change if needed.

Commented [20A76]: Change if needed.

Commented [20A77]: Change if needed.

Commented [20A78]: Change if needed.

Commented [20A79]: Adjust the frequency according to your company practices.

8. Validity and document management

This document is valid as of [date].

The owner of this document is the Incident Manager, who must check and, if necessary, update the document at least once a year.

Commented [20A80]: This is only a recommendation; you can change the frequency according to your company practices.

9. Appendices

- Appendix 1 – Incident Record
- Appendix 2 – Major Incident Report

[Job title]
[Name]

____
[Signature]

Commented [20A81]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.