Appendix 1 – Incident Response Plan

Commented [270011]: To learn how to fill out this document, and to see real-life examples of what you need to write, watch this video tutorial: "How to Write a Business Continuity Plan According to ISO 22301".

To access the tutorial: In your Inbox, find the email that you received at the moment of purchase. There, you will see a link and a password that will enable you to access the video tutorial.

Change history

Date	Version	Created by	Description of change
	0.1	27001Academy	Basic document outline

Table of contents

1. Purpose, scope and users

The purpose of this Plan is to ensure the protection of health and safety of people in the case of disaster or other incident, and to contain the incident. The objective is to reduce damage to the business to the smallest possible extent.

This Plan is applied to all major incidents threatening to disrupt any critical activity within ISMS [BCMS] scope for a period longer than the recovery point objective for each individual activity (further in text: disruptive incidents).

Users of this document are all employees of [organization name].

Commented [270012]: Include the name of your company.

2. Authorizations and responsibilities in incident response

Commented [270013]: To learn more about this topic, read this article:

Beyond the BCM Manager: Additional roles to consider during the disruptive incident https://advisera.com/27001academy/blog/2016/12/05/beyond-the-bcm-manager-additional-roles-to-consider-during-the-disruptive-incident/

Role in recovery / job title	*Authorizations and responsibilities*
Any employee	Notifying the responsible organizational unit about the incident
[job title] or team in [name of organizational unit]	All steps necessary to activate the solutions to resolve incidents related to IT and communications technology
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

Commented [270014]: E.g. Head of IT department.

Commented [270015]: E.g. Operations Officer.

Commented [270016]: Must be the person named in the Business Continuity Plan.

Commented [270017]: See also:

Activation procedures for business continuity plan http://advisera.com/27001academy/blog/2011/09/26/activation-procedures-for-business-continuity-plan/

Commented [270018]: Must be the person named in the Business Continuity Plan.

Commented [270019]: Must be named by HR manager / responsible.

3. Communication

Commented [2700110]: This section should be expanded with [illegible]

Commented [2700111]: To learn more about this topic, read this article:

Enabling communication during disruptive incidents according to ISO 22301 https://advisera.com/27001academy/blog/2016/12/19/enabling-communication-during-disruptive-incidents-according-to-iso-22301/

The following table lists responsibilities for communication (sending as well as receiving information and responding to information requests) with various types of interested parties:

	[Telephone]	[illegible]	[illegible]	[illegible]	[illegible]		
[Employees]							
[Owners / shareholders]							
[illegible]							

Commented [2700112]: Copy responsibilities from the [illegible] "Spokesperson" should be entered in that field.

The communication procedure is as follows:

1. Any employee who receives a communication request or wants to initiate communication [redacted]
2. [redacted] misinformation.
3. [redacted]
4. [redacted] party.

[redacted] any interested party.

4. Procedures for disruptive incidents

4.1. Managing a disruptive incident

[redacted]

[redacted]

[redacted]

[redacted] or the Crisis Manager.

In case an incident occurs, employees can freely communicate only with their relatives and the [redacted]

4.1.2. Disruptive incident handling

The person who received information about the incident must assess whether the incident/potential [redacted]

Commented [2700113]: Must be the person named in Business Continuity Plan.

Commented [2700114]: Include here all incidents identified as most probable during risk assessment.

Commented [2700115]: [redacted]

Commented [2700116]: E.g. Head of IT department.

Commented [2700117]: E.g. Operations Officer.

Commented [2700118]: [redacted]

- [redacted] document
- [redacted] responsibility
- notify [job title], who must consider whether any of the interested parties need to be alerted
- [redacted]

Commented [2700119]: E.g. Business Continuity Manager, Security Manager, Information Security Manager, etc.

In case a person is unable to contain and/or eradicate the incident, he/she must inform the Crisis [redacted]

[redacted] Incident Log.

4.1.3. Crisis Manager

The Crisis Manager must monitor the progress of incident handling and the period of disruption of [redacted]

[redacted] must notify all recovery managers who will have to activate their recovery plans.

4.2. Containing and eradicating an incident

Commented [2700120]: This chapter only provides procedures [redacted]

[redacted]

[redacted] appended to the Business Continuity Plan.

Crisis Manager	• In case people's lives or health are threatened, issue an evacuation order • [redacted] • [redacted] responsible for executing evacuation
[redacted]	[redacted]
All employees	• Evacuate in accordance with evacuation plans for your building • [redacted] • [redacted] • [redacted]

	items with you • [illegible]
Crisis Management Support Team	• [illegible] and missing persons

[illegible]

[illegible]

[illegible]	• [illegible] • [illegible]

[illegible]

[illegible]	• [illegible]
[illegible]	• [illegible]
All employees	• In line with the recovery plans, proceed with alternative ways of executing activities, without the use of electricity
Employees in [IT department name]	• Monitor UPS devices and execute information system shutdown as necessary

Commented [2700121]: E.g. facilities analyst, facilities technician, etc.

4.2.4. Earthquake

[illegible]

[illegible]	• [illegible] • [illegible] • [illegible] • [illegible] • [illegible]
[illegible]	• [illegible]
Crisis	• Shut down all utilities - gas, electricity, heating, ventilation, water supply

Management Support Team	• Secure the building and other property

4.2.5. *Threat letter*

All employees	• [redacted] • [redacted] • Notify [job title] • Proceed according to instructions by [job title]
[job title] or designated team	• Notify the police on [telephone number] • Notify the superior of the employee who reported about the letter • Execute measures as instructed by police

Commented [2700122]: E.g. Security Officer.

Commented [2700123]: E.g. Security Officer.

Commented [2700124]: E.g. Security Officer.

4.2.6. *Threat call / bomb threat*

All employees	• [redacted] • [redacted] • Allow the caller to say as much as possible, without interruptions: [redacted] - repeat each request made by the caller • [redacted] - Where is it located? [redacted] • Open office doors only if you are sure that they are not wired to the bomb • [redacted] • [redacted] • [redacted]
Crisis Manager	• Notify the responsible person in the organizational unit targeted by the [redacted] • [redacted] • [redacted] point should be at least 300 meters away • Notify persons responsible for evacuation and the Crisis Management

	Support Team about the new assembly point location - [redacted]

4.2.7. *Telecommunications failure*

Employees in [Department name]	- Any employee receives information about the failure - [redacted]
Employees - users of communications services	- Use alternative means of communication

Commented [2700125]: These are responsibilities of the department for Information Technology (IT). Please include the term that you use for the IT department in your company.

4.2.8. *Information system failure*

Employees in [Department name]	- [redacted] incident
Crisis Manager	- Consultation with all relevant services, assessment of incident severity
All employees	- If possible, proceed to alternative ways of carrying out activities

Commented [2700126]: These are responsibilities of the department for Information Technology (IT). Please include the term that you use for the IT department in your company.

4.2.9. *Malicious code attack*

Employees in [Department name]	- [redacted] responsible for information security] should be notified - [redacted] person responsible for IT in that organization - [redacted] - As needed, coordinate the process with IT service providers
All employees	- [redacted] - do not shut down the network devices and servers - this is the job of people from [Department name]
Employees in [Department name]	- If the computer is still not disconnected from the network, assess whether to [redacted] - Close your software (including the operating system) - for servers, assess

Commented [2700127]: These are responsibilities of the department for Information Technology (IT). Please include the term that you use for the IT department in your company.

Commented [2700128]: These are responsibilities of the department for Information Technology (IT). Please include the term that you use for the IT department in your company.

Commented [2700129]: These are responsibilities of the department for Information Technology (IT). Please include the term that you use for the IT department in your company.

	whether system users should be notified first • [illegible] • [illegible]

4.2.10. Violation of internal or external rules

[job title]	• [illegible]

5. Managing records kept on the basis of this document

Record name	***Storage location***	***Person responsible for storage***	***Controls for record protection***	***Retention time***
Incident log	Shared folder on the intranet	[job title]	Only [job title] has the right to edit the list	3 years

Commented [2700130]: Insert the data in this column to reflect your real needs.

Commented [2700131]: E.g. Incident Manager, incident analyst who received the incident report, etc.

Commented [2700132]: E.g. Incident Manager, Security Officer, etc.

Only [job title] can grant other employees access to the records.

6. Validity and document management

This document is valid as of [date].

This document, together with all additional materials, is stored in the following way:

- [illegible]
- [illegible]

Commented [2700133]: Store the document to enable access only to authorized persons.

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

Commented [2700134]: This is only a recommendation; adjust frequency as appropriate.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

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

[job title]
[name]

____
[signature]

Commented [2700135]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.