[Organization logo]

[Organization name]

BUSINESS CONTINUITY PLAN

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

Commented [270012]: All fields in this document marked by square brackets [ ] must be filled in.

Commented [270013]: Learn more in this article:

Business continuity plan: How to structure it according to ISO 22301
http://advisera.com/27001academy/knowledgebase/business-continuity-plan-how-to-structure-it-according-to-iso-22301/

Commented [270014]: 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	27001Academy	Basic document outline

Table of contents

1. Purpose, scope and users

The purpose of the Business Continuity Plan is to define precisely how [organization name] will manage incidents in the case of a disaster or other disruptive incident, and how it will recover its activities within set deadlines. The objective of this plan is to keep the damage of a disruptive incident at an acceptable level.

Commented [270015]: Insert the name of your company.

This plan is applied to all critical activities inside the scope of the Information Security Management System (ISMS) [Business Continuity Management System (BCMS)].

Commented [270016]: This is to be inserted instead of the ISMS in case the project involves only the BCMS.

Users of this document are all staff members, both inside and outside the organization, who have a role in business continuity.

2. Reference documents

- ISO 22301 standard, clause 8.4
- ISO 27001 standard, clause A.5.29
- List of Legal, Regulatory, Contractual and Other Requirements
- Business Continuity Policy
- Business Impact Analysis questionnaires
- Business Continuity Strategy

Commented [270017]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "03_Identifictation_of_Requirements".

3. Business Continuity Plan

3.1. Plan content

The Business Continuity Plan consists of these major parts:

- Business Continuity Plan – defines top-level rules for business continuity
- [illegible]
- [illegible]
- [illegible] each activity

Each of these plans defines its activation procedure.

3.2. Assumptions

[illegible] Strategy need to be prepared.

Commented [270018]: Alternatively, you can define what [illegible]

3.3. Appointments and authorities

The following bodies are formed when a disruptive incident occurs:

[redacted]		
Members:	[redacted]	[redacted]
CEO	[redacted]	[redacted]
Business Continuity Manager	IT Manager	Coordinate IT tasks from Business Continuity Plan
[redacted]		
Members:	[redacted]	[redacted]
CEO assistant	[redacted]	[redacted]
Courier	[redacted]	[redacted]

The purpose of the Crisis Management Team [redacted] responsible to the Crisis Management Team.

[redacted]

Authorizations for action during disruptive incident are the following:

[redacted]	***Who is authorized***
How small incidents related to IT and communications technology are resolved	Employees in [name of organizational unit]
[redacted]	Employees in [name of organizational unit]
Making a decision about invoking recovery plans	Crisis Manager
[redacted] site (use of close or remote alternative site)	Crisis Manager
Informing employees about the invocation of recovery plans	[redacted] recovery manager for individual activity
[redacted] individual activities	[redacted]
[redacted] parties	Crisis Manager
[redacted] media during disruptive incident	[job title]

Commented [270019]: 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/

Commented [2700110]: List all names.

Commented [2700111]: Describe briefly the duties of each

Commented [2700112]: [redacted]

Commented [2700113]: These are just examples please change this information according to your company practice.

Commented [2700114]: E.g. IT department.

Commented [2700115]: E.g. Operational department.

Commented [2700116]: E.g. Public Relations Officer.

Purchases during disruptive incident - over [amount]	[job title]
Purchases during disruptive incident - up to [amount]	[job title]

[illegible]

[illegible] been contained or eradicated.

[illegible] longer than the recovery time objective for that activity. The decision of the Crisis Manager may be written or oral.

[illegible] activities.

3.5. Communication

The following means will be used for communication between the Crisis Management Team and [illegible] from the list is to be used first; in case it is not available, the next one is used):

1. [illegible]
2.

[Job title] in the Crisis Management Team is responsible for coordinating communication with all activities.

[illegible] specified in the Incident Response Plan.

[illegible]

[illegible]

[illegible] Plan.

3.7. Order of recovery for activities

Activities must be recovered in the following order:

No.	*Name of activity*	*Recovery time objective*

Commented [2700117]: E.g. CEO.

Commented [2700118]: E.g. Procurement manager.

Commented [2700119]: To learn more about this topic, read this article:

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

Commented [2700120]: 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/

Commented [2700121]: [illegible]

Commented [2700122]: E.g. Business Continuity Manager, Security Manager, Information Security Manager, etc.

Commented [2700123]: E.g. Facilities officer.

Commented [2700124]: Fill in this table by copying the information from the Business Continuity Strategy.

Typically, IT department will have the shortest recovery time objective.

1	IT Department	4 hours
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

Commented [2700125]: These are just examples. Change this information according to your company practice.

[illegible]

[illegible] for activities.

3.9. Required resources

[illegible] Recovery Plan.

[illegible] Team, is equipped as follows:

Commented [2700126]: Copy from Business Continuity Strategy.

Commented [2700127]: [illegible]

Commented [2700128]: This column is used to write down [illegible]

Name of resource	[illegible]	[illegible]	[illegible]	[illegible]
Applications / databases:				
Data in electronic form:				
Business Continuity Strategy and plans for all activities			[illegible]	
Data in paper form:				
Business Continuity Strategy and plans for all activities			[illegible]	

IT and communications equipment:				
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
External services:				
Electricity			immediately	

4. Restoring and resuming business activities from temporary measures

[illegible] disruptive incident.

[illegible] activate each of the following steps is made by the Crisis Manager.

The following steps need to be performed, in this order:

1. [illegible]
2. [illegible]
3. Developing an action plan – determining the steps needed to return activities to normal state

4.1. Preservation of damaged assets and evaluation of damage

[illegible] prevent the damage from spreading.

Commented [2700129]: E.g. Business Continuity Manager, Security Manager, Information Security Manager, etc.

[Job title] will nominate the team for evaluation of damage. The evaluation must consist of the [illegible]

Commented [2700130]: E.g. Business Continuity Manager, Security Manager, Information Security Manager, etc.

Commented [2700131]: [illegible]

4.2. Assessment of the situation & determining options and responsibilities

Depending on the extent of the damage, the Crisis Manager needs to decide the following: (1) [illegible] whether there are enough human resources to support normal operations, etc.

Based on these decisions the Crisis Manager must nominate responsible persons for the following:

a) Making claims against insurance policies
b) [illegible]
c) [illegible]
d) [illegible]
e) [illegible]
f) [illegible]
g) [illegible]
h) [illegible]

4.3. Developing action plans

[illegible] resources, (3) required financial resources, and (4) deadlines.

[illegible] perform the review of the steps once they are completed.

5. Validity and document management

This document is valid as of [date]

This document is stored in the following way:

- [illegible]
- [illegible]

Commented [2700132]: It is usually stored at all alternative [illegible]

Commented [2700133]: Store the document to enable access [illegible]

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.

[illegible] considered:

- Did activities recover within required time?
- [illegible]
- [illegible]

6. Appendices

- Appendix 1 – Incident Response Plan
- [illegible]
- [illegible]
- Appendix 4 – Transportation Plan
- [illegible]
- [illegible]
- Appendix [number] – Activity Recovery Plan for [name of activity]

Commented [2700135]: List separately for each activity.

[job title]
[name]

____
[signature]

Commented [2700136]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.