[Organization logo]

[Organization name]

BUSINESS CONTINUITY STRATEGY

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 about the business continuity strategy here:

Can business continuity strategy save your money?
https://advisera.com/27001academy/blog/2010/03/15/can-business-continuity-strategy-save-your-money/

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 this document is to define which options and solutions [organization name] will ensure that all conditions for the resumption of business activities in the case of disaster or other disruptive incident are met. It forms the basis for preparing the Business Continuity Plan and recovery plans.

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

This document is applied to the entire BCMS scope as defined in the Business Continuity Management Policy.

Users of this document are members of top management and persons implementing the business continuity management project.

2. Reference documents

- ISO 22301 standard, clauses 8.3 and 8.4.2
- ISO 27001 standard, clauses A.5.5 and A.5.29
- Business Continuity Management Policy
- Business Impact Analysis questionnaires
- [Risk assessment document]
- [Risk treatment document]
- Business Continuity Plan containing the Incident Response Plan and recovery plans.

3. Strategy input

This Strategy and related solutions are written based on Business Impact Analysis results and results of risk assessment and risk treatment.

Commented [270016]: Solutions refers to organizational (E.g. [illegible]

3.1. Business Impact Analysis

[illegible]

Commented [270017]: Include here the number of the [illegible]

[illegible] Recovery Time Objectives for Activities to see the consolidated results.

[illegible] activity, taking into account dependencies on other activities.

Commented [270018]: To learn more about this topic, read this article:

What is the difference between Recovery Time Objective (RTO) and Recovery Point Objective (RPO)? https://advisera.com/27001academy/knowledgebase/what-is-the-difference-between-recovery-time-objective-rto-and-recovery-point-objective-rpo/

3.2. Risk management

Commented [270019]: To understand the difference between business impact analysis and risk management, read this article:

Risk assessment vs. business impact analysis https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/#section23 [illegible] assessment are the following:

- [illegible]

For all mentioned risks / incidents it is necessary:

- [illegible]
- [illegible]
- [illegible] point for exercising and testing plans
- to define in the Incident Response Plan the appropriate way to respond to each of the incidents

[illegible] the Incident Response Plan.

4. Incident response structure

4.1. Crisis Management Team and Crisis Management Support Team

[illegible]

[illegible] Management Team are:

- [all members of the top management]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

[illegible] Centre, the location of which is specified in item 5.1 of this Strategy.

4.1.2. Crisis Management Support Team

Commented [2700110]: Include the name of the Risk assessment document referred to in section 2.

Commented [2700111]: [illegible]

Commented [2700112]: [illegible]

Commented [2700113]: [illegible]

Commented [2700114]: E.g. Business Continuity Manager, Information Security Manager, Security Manager, etc.

Commented [2700115]: E.g. Business Continuity Manager, Information Security Manager, Security Manager, etc.

Commented [2700116]: [illegible]

Commented [2700117]: To learn more about incident management structures, read this article:

Incidents in ISO 22301 vs. ISO 27001 vs. ISO 20000 vs. ISO 28003
https://advisera.com/27001academy/blog/2016/09/05/incidents-in-iso22301-vs-iso27001-vs-iso-20000-vs-iso28003/

Commented [2700118]: 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 [2700119]: Adapt to the organization's standard naming system.

Commented [2700120]: Assess whether these are the best [illegible]

Commented [2700121]: This is usually someone with appropriate seniority and high level of authority.

[illegible] incident.

Members of the Crisis Management Support Team are:

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

The Crisis Management Support Team shall work on locations specified by the Crisis Management Team.

[illegible]

[illegible] must be equipped as follows:

Name of resource	Description	[illegible]	[illegible]
Applications / databases:			
[illegible]			
[illegible]			[illegible]
[illegible]			
[illegible]			[illegible]
[illegible]			
[illegible]			[illegible]
[illegible]			[illegible]
[illegible]			[illegible]
[illegible]			[illegible]
[illegible]			[illegible]
Communication			

Commented [2700122]: Adapt to the organization's standard naming system.

Commented [2700123]: These are only examples. You can delete or add new based on your company practice.

Commented [2700124]: Depending on the number of [illegible]

channels:			
[illegible]			[illegible]
[illegible]			[illegible]
[illegible]			
[illegible]			[illegible]
[illegible]			[illegible]
[illegible]			
[illegible]			
[illegible]			[illegible]
[illegible]			[illegible]
External services:			
Electricity			immediately

[illegible] Command Centre.

4.2. Reporting and decision making

Incidents are reported in the following way:

- [illegible]
- [illegible]

If the persons mentioned are unable to resolve the incident, they must inform the Crisis Manager [illegible]

[illegible]

[illegible]	***Who is authorized***
[illegible] technology are resolved	Employees in [name of organizational unit]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
Purchases during disruptive incident - over [amount]	[job title]
Purchases during disruptive incident - up to [amount]	[job title]

Commented [2700125]: E.g. Business Continuity Manager, Security Manager, business unit responsible, process owner, etc.

Commented [2700126]: This is usually someone with appropriate seniority and high level of authority.

Commented [2700127]: [illegible]

Commented [2700128]: E.g. Head of IT department.

Commented [2700129]: E.g. Security Officer.

Commented [2700130]: [illegible]

Commented [2700131]: E.g. Purchase manager.

Commented [2700132]: E.g. Purchase analyst.

[illegible] preparing employees in [name of organizational unit] to handle other incidents.

4.3. Cooperation with authorities

The following persons are in charge of coordination with state authorities and emergency services:

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

[illegible] disruptive incident and how the organization is expected to react.

[illegible]

[illegible]

After evacuating the building employees must gather at the following assembly points:

	[illegible]	[illegible]
[address of location no. 1]		
[address of location no. 2]		
[address of location no. 3]		
[address of location no. 4]		

[illegible]

[Job title] is responsible for preparing and maintaining evacuation plans in the case of fire.

4.5. Means of communication

[illegible] top of the list are to be used first, those near the bottom are used only if the former are out of order:

1. [illegible]
2. [illegible]
3. [illegible]
4. [messaging services - e.g. Skype]
5. [illegible]
6. [illegible]
7. [illegible]

Commented [2700133]: E.g. Head of IT department.

Commented [2700134]: E.g. Business Continuity Manager.

Commented [2700135]: List other authorities relevant for the work of the organization, if any – e.g. national or regional threat advisory system.

Commented [2700136]: If such a plan does not exist, it is necessary to provide here more details on how the building is evacuated.

Commented [2700137]: [illegible]

Commented [2700138]: E.g. Business Continuity Manager, business unit responsible, facilities manager, EHS manager, etc.

Commented [2700139]: 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/

8. [satellite phones - state where they are stored and who has a right to use them]

[illegible] means of communication to ensure they are available during a disruptive incident.

[illegible]

[illegible] following ways:

[illegible]	[illegible]
[illegible]	[illegible]
[activity]	

[Job title] is responsible for providing for all means of transportation.

[illegible]

[illegible] communicate with them in the case of disruptive incident by the following means of communication:

	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		
[Employees]							
[Owners / shareholders]							
[Employees' relatives]							
[Clients]							
[Public media]							
[Associations]							
[Emergency services]							
[various state authorities]							

[illegible] disruptive incident.

[Job title] is responsible for preparing templates for the media statements, which would cover all disruptive incidents related to the above-mentioned highest risks.

Commented [2700140]: These are only examples. You can [illegible] defined.

Commented [2700141]: E.g. Business Continuity Manager, business unit responsible, facilities manager, etc.

Commented [2700142]: An appropriate way of transportation must be selected for each critical activity.

Commented [2700143]: List all activities.

Commented [2700144]: E.g. facilities manager

Commented [2700145]: Include the name of your company.

Commented [2700146]: [illegible]

Commented [2700147]: E.g. Business Continuity Manager.

Commented [2700148]: E.g. Business Continuity Manager, Communication Manager, Public Relation

5. Resource Strategy

5.1. Sites and infrastructure solutions

Recovery sites of [organization name] are the following:

Name	[illegible]	[illegible]	***Min. number of workplaces***	[illegible]	[illegible]	***Alternative site – remote***
Command Centre	[address]	[illegible]		[illegible]	[illegible]	[illegible]

Commented [2700149]: Include the name of your company.

Commented [2700151]: This site is usually in the same city/area as the primary site.

Commented [2700150]: Depending on the number of people in a critical activity.

Commented [2700152]: This site is usually located at least 40 km from the primary site. Read also this article:

Disaster recovery site – all you need to know
https://advisera.com/27001academy/knowledgebase/disaster-recovery-site-what-is-the-ideal-distance-from-primary-site/

		organization in the case of disaster); d) alternative sites provided by specialized organizations (e.g. organizations which rent their facilities for the case of disaster, but also hotels or, for example, educational institutions equipped with IT infrastructure); e) working at home or at some other remote location (such an option is possible for activities that do not require access to physical documentation, infrastructure, etc.)]				
[name of activity]	[address]				[address]	[address]

Commented [2700153]: Select for each critical activity and Crisis Management Team at least one of the strategies mentioned.

Commented [2700154]: List all activities, including the activity responsible for central IT infrastructure.

*Terms used in this column have the following meaning:

a) [redacted]
b) [redacted]
c) [redacted]
d) [redacted] and real time data

[Job title] is responsible for making all necessary arrangements concerning alternative sites. [Job title] is responsible for equipping alternative sites.

Commented [2700155]: E.g. facilities manager

Commented [2700156]: E.g. IT manager, operations manager, facilities manager, etc.

5.2. Suppliers and outsourcing partners solutions

Relations with suppliers and outsourcing partners must be managed in the following way:

Name of supplier / outsourcing partner	[illegible]
	[illegible]

Commented [2700157]: [illegible]

Commented [2700158]: Select one or more of the listed [illegible]

[illegible] interoperability during disruptive incident is at a satisfactory level.

Commented [2700159]: E.g. Purchase manager, facilities manager.

[illegible]

[illegible] not required within 24 hours, the installation media will be stored at the alternative site.

[Job title] is responsible for application/database installation and/or for the preparation of installation media.

Commented [2700160]: E.g. IT manager.

5.4. Data solutions

Backup copies of data shared by several activities must be made at following intervals:

[illegible]	[illegible]	[illegible]
		[illegible] them and storing at two separate locations]

[illegible] strategy for the said activity.

[Job title] is responsible for creating backup copies of the above-mentioned data.

5.5. Avoiding a single point of failure

The following strategies are used to avoid a single point of failure which can cause a disruption of an activity:

[illegible]	[illegible]	[illegible]

[Job title] is responsible for implementing the single point of failure avoidance strategy.

[illegible]

[illegible] [amount in local currency] for urgent purchases in case a disruptive incident occurs.

Commented [2700161]: Copy from Business Impact Analysis Questionnaire.

Commented [2700162]: [illegible]

Commented [2700163]: Depending on the type of data, select appropriate strategy; add other strategies if necessary.

Commented [2700164]: If there are several groups of data, [illegible]

Commented [2700165]: Copy from Business Impact Analysis Questionnaire.

Commented [2700166]: Plan for alternative or backup resources, creation of backup copies, precise contractual obligations with suppliers, etc.

Commented [2700167]: If there are several types of single [illegible]

Commented [2700168]: Include the name of your company.

Commented [2700169]: Calculate from Business Impact Analysis Questionnaires.

Commented [2700170]: [illegible] are to be purchased immediately or shortly after an incident occurs.

[illegible] provide private loan; or (d) [names of suppliers and outsourcing partners] will extend the payment terms.

Commented [2700171]: Specify other financial instruments that can be liquidated in very short time.

[illegible] resources.

Commented [2700172]: This is usually someone with appropriate seniority and high level of authority.

[illegible]

[illegible]

[illegible] Recovery Plans for this activity. [Job title] is responsible for preparing all resources necessary for individual activities.

Commented [2700173]: This is usually someone with appropriate seniority and high level of authority.

[illegible]

[illegible] implementation of each preparation; [job title] is in charge of monitoring coordination and execution of all preparatory actions, as well as of reporting about their implementation.

Commented [2700174]: This is usually someone with appropriate seniority and high level of authority.

Commented [2700175]: E.g. Business Continuity Manager, Security Manager, etc.

8. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Preparation Plan for Business Continuity (in electronic form)	Computer of [job title responsible for monitoring execution]	[job title responsible for monitoring execution]	Only [job title] has the right to make entries and changes to Plan data.	The Plan is stored for the period of 3 years

Commented [2700176]: Insert the data in this column to reflect your real needs.

Commented [2700177]: E.g. Business Continuity Manager, Security Manager, etc.

9. Validity and document management

This document is valid as of [date].

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

Commented [2700178]: E.g. Business Continuity Manager, Security Manager, etc.

Commented [2700179]: 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]

10. Appendices

- [illegible]
- [illegible]
- [illegible]
- Appendix [number] – Activity Recovery Strategy for [name of activity]

Commented [2700180]: Insert for each critical activity, starting from Appendix 4.

[job title]
[name]

____
[signature]

Commented [2700181]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.