Appendix 6 – Disaster Recovery Plan

Commented [270011]: To learn more about Disaster recovery plans, read this article:

Disaster recovery vs business continuity
https://advisera.com/27001academy/blog/2010/11/04/disaster-recovery-vs-business-continuity/

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 Disaster Recovery Plan is to define precisely how [organization name] will recover its IT infrastructure and IT services within set deadlines in the case of a disaster or other disruptive incident. The objective of this Plan is to complete the recovery of IT infrastructure and IT services within the set recovery time objective (RTO).

This Plan includes all resources and processes necessary for the recovery.

Users of this document are members of the Crisis Management Team and employees' necessary for the recovery of this activity.

Commented [270012]: This plan is written for organizations where the recovery of IT infrastructure and IT services can be fitted into a single plan.

For organizations that have complex IT infrastructure, or have different RTOs for different IT systems, it might be better to develop separate Disaster Recovery Plans for different IT systems.

2. Reference Documents

- ISO/IEC 27001 standard, clauses 7.4, A.5.29, A.5.30, and A.8.14
- ISO 22301 standard, 8.4.5
- [List of Legal, Regulatory, Contractual and Other Requirements]
- [Incident Management Procedure]
- [Internal Audit Procedure]

Commented [270013]: If you don't have this List, then in these bullets list all the legislation and contracts that contain requirements for access control.

3. Assumptions / limitations

In order for this plan to work, the following conditions must be met:

- [illegible] Strategy.
- [illegible] the alternative site – this is the starting point for this Disaster Recovery Plan.

Commented [270014]: [illegible]

This plan does not cover the following types of incidents:

-

Commented [270015]: You can specify here some incidents that this plan would not be able to mitigate – e.g., larger earthquake.

4. General information

Location of the alternative site / recovery strategy	
[illegible]	[illegible]

Commented [270017]: Copy from the Business Continuity Strategy.

E.g. street, number, ZIP-Code, etc.

Commented [270016]: To learn more about this topic, read 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/

Commented [270018]: [illegible]

Commented [2700110]: [illegible]

activation:	
[illegible]	[illegible]
[illegible]	[illegible]
Key tasks / obligations / SLAs that must be fulfilled and respective deadlines:	
[illegible]	[illegible]

Commented [270019]: 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 [2700111]: Usually all employees of the IT department.

Commented [2700112]: Usually the Head of the IT department.

Commented [2700113]: Usually the Head of the IT department.

Commented [2700114]: The usual criteria is that all conditions have been met to resume the provision of IT services to the business users.

Commented [2700115]: Copy from the strategy for the IT department.

E.g. Recover financial process in 8 hours, according SLA XX/20YY.

Commented [2700116]: [illegible]

Commented [2700117]: [illegible]

5. Roles and contact information

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/

For IT department:

No.	***Role in recovery***	[illegible]
1.	*e.g. Database recovery*	
2.	*e.g. Application recovery*	
3.		
4.		

Commented [2700119]: In case there is no business mobile phone, use private one.

Commented [2700120]: [illegible]

Commented [2700121]: These are just examples please change this information according to your company practice.

5.								

Other activities in the company:

No.	Name					
11.						
12.						
13.						
14.						
15.						

Commented [2700122]: I.e., business departments in the company.

Use the data from the previous section as examples.

External contacts:

No.	Name of organization						
21.							
22.							
23.							
24.							
25.							

Commented [2700123]:

Use the data from the previous section as examples.

6. Authorizations in a crisis

Role in recovery / job title	
Head of IT department	
[job title]	
[job title]	
[job title]	
[job title]	
...	

Commented [2700124]: To fill in this table, copy the information from the Business Continuity Strategy.

Commented [2700125]: E.g. Purchase Manager.

Commented [2700126]: E.g. CEO, Marketing Manager

Commented [2700127]: E.g. CEO, Business Continuity Manager, Security Manager, Information Security Manager, etc.

Commented [2700128]: E.g. Senior System Admin, Senior Database Admin, etc.

Commented [2700129]: List all other necessary authorizations outside the normal area of responsibility.

Note: Only [job title] is authorized to communicate with the public through public media.

Commented [2700130]: Usually someone from the Crisis Management Team.

7. Necessary resources

The following resources will be used for the recovery of this activity:

Name of resource				

Commented [2700131]: To fill in this table, copy the information from the Business Continuity Strategy.

Commented [2700132]: Describe where resources are located, etc.; for external services list suppliers.

Commented [2700133]:

People:				
Applications / databases:				
[redacted]				
Facilities and infrastructure:				
E.g. Computer network			*E.g. within 2 hours*	
E.g. Furniture			*E.g. immediately*	

Commented [2700134]: In particular, list all the backup data together with its location and the way to access this backup data.

External services:				
E.g. Electricity			*E.g. immediately*	

8. Recovery steps for the IT infrastructure / IT services

This activity must be recovered in the following way:

Recovery procedures (main steps / individual tasks)			
[name of step no. 1]			
[task no. 1.1]			
[task no. 1.2]			
...			
[name of step no. 2]			
[task no. 2.1]			
[task no. 2.2]			
...			

9. Managing records kept on the basis of this document

Record name	***Storage location***	***Person responsible for storage***	***Controls for record protection***	***Retention time***
Record of recovery step implementation (record in paper form)	Archive [job title]	[job title]	Records are stored in a locked cabinet	3 years

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

10. Validity and document management

This document is valid as of [date].

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

Commented [2700135]: Make sure you list all the services that will be necessary for the recovery of your IT infrastructure and IT services.

Commented [2700136]: To learn more about this topic, read this article:

Understanding IT disaster recovery according to ISO 27031
https://advisera.com/27001academy/blog/2015/09/21/understanding-it-disaster-recovery-according-to-iso-27031/

Commented [2700137]:

Commented [2700138]: This column is filled in only in the event the plan is activated.

Commented [2700139]:

Commented [2700140]: Insert the data in this column to reflect your real needs.

Commented [2700143]: Usually the Business Continuity Coordinator.

Commented [2700142]: Usually the Business Continuity Coordinator.

Commented [2700141]: Alter this record to match what you already have in your company. If you do not have a similar record, you can create a new one in the format that suits you best.

- The paper form of the document is stored at the following locations: Command Center, [list locations].
- [illegible]

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

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

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

11. Additional documents

- [illegible]
- [illegible]

[job title]
[name]

_____
[signature]

Commented [2700144]: It is usually stored at the disaster recovery alternative site.

Commented [2700145]: Store the document to enable access only to authorized persons.

Commented [2700146]: E.g. Business Continuity Manager, Security Manager, etc.

Commented [2700147]: This is only a recommendation; adjust frequency as appropriate.

Commented [2700148]: [illegible]

Commented [2700149]: [illegible]

Commented [2700150]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.