‘<Subject>’

(Disaster) Recovery/Contingency Plan

Implementing a contingency solution can be documented in a similar way as a recovery plan. Just replace the word ‘recovery’ to ‘contingency’.

As there is no strict recommended way to document these plans, this template simply provides ideas and considerations.

|  |  |
| --- | --- |
| Document Management | |
| **Version:** | V0.1 |
| **Date Issued:** | XX |
| **Owner:** | XX |
| **Change Manager:** | XX |
| **Governance Forum** | XX |

Contents

[1 Introduction 4](#_Toc106973038)

[1.1 Purpose of this recovery plan and scope 4](#_Toc106973039)

[1.2 Location of this document 4](#_Toc106973040)

[1.3 Maintenance of this document 4](#_Toc106973041)

[1.4 Acronyms 4](#_Toc106973042)

[2 Recovery Protocol 5](#_Toc106973043)

[2.1 Authorisation, qualified team, and coordination 5](#_Toc106973044)

[2.2 Check if recovery is required 5](#_Toc106973045)

[2.3 Communicate commencement 5](#_Toc106973046)

[2.4 Perform Recovery 5](#_Toc106973047)

[2.5 Verify Recovery 5](#_Toc106973048)

[2.6 Communicate completion 5](#_Toc106973049)

[2.7 Post recovery review, lessons learned and plan update 6](#_Toc106973050)

[3 Recovery Procedure 6](#_Toc106973051)

[4 APPENDIX A: When and how to make plans 7](#_Toc106973052)

Template Overview

This document is a template and the use of it is not mandatory.

Texts can be an explanation, or it can be example text. Modify and adjust it according to your needs. You can reuse text, modify, or replace it. Also, chapters, headers and appendices can be changed.

Response, contingency, and recovery plans will require **different structures and different content, depending on the subject matter** at hand. Therefore, this document **gives only a few suggestions** on how to structure your plan. It also does not mean that following the structure of the plan, that this will lead to a complete and optimal structure for your needs.

Use texts, tables and diagrams **as suit your needs**. Also consider timing of activities and events.

Consider the fact that the team(s) already will be under stress and to make the plan **easy to follow, logical and where possible, visual.** Do not be afraid to have some redundancy in the plans on the various levels, specifically around communication as this can go easily wrong.

Plans can be made for a wide variety of subjects varying from recovering IT systems, to equipment, information, organisational disruptions, or third-party relationships.

Consider placing things to do and check in emergencies upfront without lengthy texts. If necessary, detail this in a separate section of the document.

Consider checking with colleagues what plans have already been made and use these as examples.

**See Appendix** A for explanation on the different types of plans.

**Remove this page after completing the document.**

# Introduction

## Purpose of this recovery plan and scope

This plan applies to [type of incidents] of [specific organisational area].

If for a specific subject, scope, or incident both a contingency plan and a recovery plan exists, it is often the same people that will need to work on both contingency implementation and recovery, and it might very well be possible that it is technically not possible or just not practical to work on the contingency implementation in parallel with the recovery. Make sure that this is communicated to stakeholders so they will know the dependency between contingency solution and recovery.

Outline this dependency here but also make sure it is documented in any existing overarching plans.

## Location of this document

The most recent final version of this document can be found on website …….

## Maintenance of this document

This document will be maintained by the Senior Program Lead, Business Continuity and Resilience under responsibility of the document owner.

## Acronyms

BCP Business Continuity Plan

BRT Business Response Team

CMP Crisis Management Plan

CMT Crisis Management Team

DRP Disaster Recovery Plan

IRP Incident Response Plan

IRT Incident Response Team

# Recovery Protocol

The following paragraphs describe the protocol that the recovery is subject to. The actual recovery steps are documented in the subsequent chapter(s).

Depending on the amount of text required to describe this protocol, consider using a table or flow diagram to describe the protocol.

## Check if recovery is required, impact assessment and escalation

Before you start with the recovery, double check to see if the recovery is actually required and that no one else has already started the recovery. Include all prerequisites to start the recovery.

Describe the steps to perform for this check. If this is elaborate, consider a dedicated chapter.

Do an assessment of the impact of the incident to the broader organisation and its stakeholders. Understand which stakeholders are impacted and with whom communication and alignment is required.

Does the incident need to be escalated, by whom and to whom?

## Authorisation, qualified team, and coordination

Describe who can authorise the recovery.

Describe who can perform the recovery. If it is a team, describe the team structure, roles, etc. If specific skills and knowledge are expected, describe those.

Describe how the activities will be coordinated. Think about shared workspaces (virtual and physical), meetings, meeting rooms, Zoom details, etc.

## Communicate commencement

Communicate to stakeholders that you start the recovery. If this is normally not expected of the recovery person or team, a simple question to the person who authorises the recovery might be warranted. In other cases, a more elaborate communication task might be applicable.

Describe what will need to be communicate, to which stakeholders, by whom and if necessary, via what channel/mechanism.

## Perform Recovery

These are all in the individual steps as outlined in the subsequent chapters.

Consider communicating progress during the recovery phase and if this is a considerable task, consider developing a communication protocol (e.g., who to communicate what to, when and by whom).

Consider maintaining a log of recovery steps, outcomes, etc.

## Verify Recovery

After recovery, verify that it was successful. In some cases, this is an elaborate check with many steps to go through but in other cases it is so obvious that not really a check is required.

The description of the verification can also be included as the last steps as part of the recovery procedure.

## Communicate completion

Once completed, communicate the results to the stakeholders.

Describe who will do this and who the stakeholders are.

## Post recovery review, lessons learned and plan update

Once completed and communicated, considering holding a review meeting to capture lessons learned and improve the plan.

# Recovery Procedure

Describe all the steps to recover, what the priorities are, and which role will perform which step.

Incidents can vary so there might be different recovery scenarios.

If required, use multiple chapters.

For the more specific plans, detail them sufficiently so that anyone with the prerequisite skills can do the recovery. Do not assume people will know the specific intricacies of the subject matter at hand. When you write this, keep a new but skilled colleague in mind who just started at the University.

If there are items that are time dependent or dependent on external parties or events, make those clear.

Do not include security codes in this document. This allows the document to be shared with a wider group, besides the fact that it is advised never to put security codes, passwords, etc. into a document. These are better secured in vaults. However, if these codes are required for recovery, make it clear who will have access to the vault or security codes.

The procedure will specify the recovery steps. This can be done as numbered list/table of steps, flow diagrams, schematics (e.g., Ikea-like instructions), photo’s, videos, scripts, etc. Where applicable give examples but make it clear that these are examples.

Refer to any existing guides, manuals or standards as required. It is very well possible to build recovery plans in a hierarchy. An overarching master recovery plan can refer to several more detailed recovery plans for various subjects, items, etc.

If the recovery can take significant time, consider including steps to communicate progress.

If there are thresholds of unsuccessful recovery steps that mean you stop recovery, document those including subsequent steps and protocols.

Consider specifying criteria when the recovery is completed. This can specifically be relevant in cases when the assessment to this can be fluid. To decide when an IT system is fully recovered is usually easy to decide. But when an organisational process is recovered, can be more difficult to judge.

# APPENDIX A: When and how to make plans

[This appendix is a guide and can be removed when making the plan.]

An organisation can make various plans to address issues, incidents, disasters, etc. with varying levels of impact and scope.

Generally, you will want to avoid incidents by building quality into your operational procedures.

Incidents that are almost daily routine, will generally be dealt with via Standard Operating Procedures (SOP’s). Incidents that are less frequent but with higher impact, can be dealt with contingency plans or recovery plans.

Contingency plans allow for a temporary workaround until recovery has been completed. Contingency measures can be spare equipment, fall-back facilities, WFH, arrangements with agencies to quickly resource extra staff, etc. Also ‘mechanisms’ such as the call-hierarchy is a contingency measure.

Recovery plans recover the situation back to the situation as it was before but, in some cases, you might want to recover to a new, better situation. If the impact of the incident is large, the recovery plan can be called a Disaster Recovery Plan (DRP).

The greater the impact, the more coordination, communication, and control will be required. For more complex incidents, you might want to create a dedicated Incident Response Plan (IRP) that focusses on the management aspect of the incident. It will describe a dedicated coordinating team to manage not only the incident but potentially also coordinate how the impacted organisation can survive until recovery has been completed.

Incident response plans can also be made to address the coordination, command, control, and communication aspects of any possible high impact incident. You cannot always predict all possible types of incidents and build contingency and recovery plans. Therefore, with a catch-all plan, you are prepared for both the foreseen and unforeseen incidents or disasters.

Contingency and recovery plans focus on the individual steps, procedures, actions of the subject matter at hand and can go in much detail. Depending on the objective, they can give higher level instructions or very low-level technical instructions. For example, how to connect wires, which commands to enter into the computer or which values to enter into a template document. But they can also contain descriptions regarding the management and coordination aspects. It will all depend on the type of incident and what you intend to address with the plan.

A recovery procedure can be prescriptive with almost a guaranteed success (e.g., resolving a paper jam in a printer) but in other cases can be more an approach or a strategy (e.g., recovering from reputational damage). In the latter case, you might even call the document a “recovery strategy”, though in that case, you can also consider calling it an “incident response plan”.

The University also has a Crisis Management Plan (CMP) and Business Continuity Plans (BCP’s) that can be activated in case of a catastrophic impact that will lead to a crisis. The Crisis Management Plan is, by definition, University-wide. Business Continuity Plans always work under the umbrella of the Crisis Management but have a narrower scope.

Please see the “WSU Business Continuity & Crisis Management Framework” for more explanation on how the various plans work together to control continuity of the business processes of the University.

Business Continuity Plans will refer to the various incident response plans, contingency plans and (disaster) recovery plans that are relevant to control a crisis and recover from a crisis. The existence of incident response plans assists with crisis management because they provide just one level further down details on how to control and manage the situation.

The Crisis Management Plan and Business Continuity Plans are developed and maintained by the BCM Program. These are the responsibility and accountability of the BCM Program, governed as per WSU Business Continuity & Crisis Management Framework.

The response, contingency and recovery plans are developed and maintained by schools and organisational units of the University.

The BCM Program provides templates, suggestions and can provide advice, but the schools and organisational units will be responsible and accountable for developing, maintaining, and practicing/testing the plans.

Plans can be made following a structured risk analysis, for example according to the Risk Management Guidelines (see DDS), but also in line with relevant standards and methodologies that are applied in the specific area of the organisation. Or simply by asking “what can go wrong?”.

In all cases when the risk analysis according to the Risk Management Guidelines indicates the need for a risk treatment in the form of a response, contingency, or recovery plan, these should be developed, maintained, and practiced or tested.

The Business Impact Analysis (BIA) that is performed as part of the BCM Program can also indicate the need for a risk treatment in the form of a plan and then the rules as per Risk Management Guidelines apply.

Given the size of the organisation and the distributed nature of the organisation, a certain part of the organisation might be in crisis-mode while the rest of the organisation is not impacted. Therefore, it is recommended to consider if the various major organisational units might need their own crisis management plans. It just that they should not be called like that. The preferred term would be “Major Incident Response Plan”. For example,

* “Hawkesbury Campus - Major Incident Response Plan”
* “School of Business - Major Incident Response Plan”.

**Note**: Schools or organisational units might already have plans created that include “crisis management” or “business continuity plan” in their names. That is fine, as long as we don’t get confused to what plans we refer. Generally, it is preferred that “crisis management” and “business continuity plan” are only used by documents managed by the BCM Program.

The schools and business units are advised (non-mandatory) to construct names for plans according to the following concept:

|  |  |
| --- | --- |
| **Name structure** | **[subject] [criticality] [level] [action] [type]** |
| Subject | Specifies the subject/scope the plan applies to, e.g., “Flood”, “School of Business”, “Building 123”.  Subject should always be specified to avoid any confusion with other documents created for other subjects/scope. |
| Criticality | Specifies how the level criticality, e.g., “Critical”, “Major”. Or leave blank”. |
| Level | Specifies what the plan is a response to, e.g., “Disaster”, “Incident”, or blank.  Do NOT use “Crisis” or “Business Continuity”. |
| Action | Specifies the action type, e.g., “Response”, “Contingency”, “Recovery”, “Management”, “Strategy”, etc. |
| Type | Specifies the type of document, e.g., “Plan”, “Guidelines”, “Framework”, etc. |
| Examples of naming structure  (does not mean the document exists) | * Flood Recovery Plan * School of Business - Critical Incident Response Plan * ITDS Disaster Recovery Plan |

The hierarchy of documents is then, where each higher-level plan can refer to the lower-level plans and where plans at each level can be activated independently:

|  |  |  |
| --- | --- | --- |
| **Impact Level** | **Plans** | **Existing Examples** |
| University-wide Crisis | * Crisis Management Plan * Crisis Communication Plan * Business Continuity Plans | * Crisis Management Plan * Crisis Communication Plan * BCP Research * BCP Teaching * BCP University Services |
| Major/Critical Incident  (crisis with limited organisational scope and not declared as a crisis by the VC or delegates) | * Major Incident Response Plan | * Teaching & Research Technical Services – BCP Master Plan |
| Moderate or Minor Incident | * Incident Response Plan | * Teaching and Research Technical Services (TRTS) - Building Alarm Response Plan; Bldg. 24 CTN Campus * TRTS Business Recovery Response Plan – Hawkesbury Campus |
| Disruption of a specific process, activity, system, facility, equipment, stakeholder group, etc. | * Contingency Plan * Recovery Plan | * ITDS Disaster Recovery Plan |

|  |  |
| --- | --- |
| **When to use …** | **… which type plan** |
| To address command, coordination, control, and communication. To bring order into the chaos and to respond quickly and decisively. | * Response Plan |
| To describe the implementation of a temporary solution to survive until recovery has taken place. | * Contingency Plan |
| To describe steps to recover to an old or new normal. | * Recovery Plan |
| Note that it is very well possible to combine response, contingency, and recovery in a single plan. For example, the “ITDS Disaster Recovery Plan” and the “TRTS Business Recovery Response Plan – Hawkesbury Campus” combine response and recovery information. | |

And don’t forget! Plans need to be maintained and tested/practiced, to verify if they work and to build up experience.