‘<Subject>’

Incident Response Plan

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

**Contents**

[1 Introduction 5](#_Toc106357853)

[1.1 Purpose of this response plan and scope 5](#_Toc106357854)

[1.2 Location of this document 5](#_Toc106357855)

[1.3 Maintenance of this document 5](#_Toc106357856)

[1.4 Acronyms 6](#_Toc106357857)

[2 Alarm and Activation 7](#_Toc106357858)

[2.1 Alarm – what types of incidents? 7](#_Toc106357859)

[2.2 Activation 7](#_Toc106357860)

[2.3 The Incident Response Team (IRT) 7](#_Toc106357861)

[3 Command, Control and Communication 8](#_Toc106357862)

[3.1 Command 8](#_Toc106357863)

[3.2 Control 8](#_Toc106357864)

[3.3 Communication 9](#_Toc106357865)

[4 Critical Processes and Recovery Priorities 10](#_Toc106357866)

[4.1 Priorities 10](#_Toc106357867)

[4.2 Critical processes 10](#_Toc106357868)

[4.3 Contingency/recovery strategies and requirements 10](#_Toc106357869)

[4.4 Metrics 11](#_Toc106357870)

[5 APPENDIX A: When and how to make plans 12](#_Toc106357871)

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.**

CHECKLIST FIRST ACTIONS

|  |  |  |
| --- | --- | --- |
| Step | Action | Who? |
| 1 | Gather the response team   * Meeting point * Online | Chair |
| 2 | Assess the situation   * Health and safety of staff, students, and lifeforms * Type of disruption; what is disrupted? * What are the consequences (for teaching and research)? * Do we know the cause? | Team |
| 3 | Coordinate   * Inform and coordinate with other teams * Agree on priority and obtain direction on actions from controlling bodies | Chair |
| 4 | Decide on actions   * Check status staff/students/lifeforms, their health and safety and direct impact on them * Immediate actions to minimise impact and survive * Actions to recover * What teams and plans can we activate? | Team |
| 5 | Communicate   * Inform staff and students and other stakeholders * Coordinate with Crisis Communication Coordinator of the CMT | Chair |
| 6 | Implement contingency solutions and/or start recovery   * Activate available plans and solutions * Coordinate with executing teams | Team |

# Introduction

## Purpose of this response plan and scope

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

This response plan will be used to survive and recover the crucial business activities, facilities, equipment, systems, or information of the university in cases of an incident.

For the survival immediately during or after the event, contingency measures will or can be taken or specific *contingency plans* can be activated. Until recovery has been completed, you will need to survive with a reduced capability, and you will need to manage this special situation.

For the recovery to the normal situation recovery measures can be taken, documented in recovery plans. Incidents with a large impact can be called a disaster and therefore those plans are referred to as *Disaster Recovery Plans (DRP’).*

If plans or means to these contingency or recovery measures already exist, these will be mentioned in this document. But new or ad hoc measures can also be taken as is required. This document does not describe recovery procedures themselves or nor it describes how contingency measures that can be implemented.

This document describes the Command, Control and Communication to respond effectively to maximise continuation of the services and to minimise damage.

The team that is responsible for the execution of this plan is called the Incident Response Team (IRT).

You will need to get various teams (or individuals) to work on the various actions, potentially using already existing recovery plans, contingency plans, response plans, approaches, guidelines, methodologies, or practices. All under different names such as recovery teams, response teams, taskforces, working groups, business units, etc.

Incident response plans can be made at different levels of the organisation for different purposes. You can have a response plan for the whole division but also for a specific business unit, facility, campus, service, etc.

*[There is no rule that says that recovery and contingency plans need to be separate documents. See Appendix A for explanation on types of documents.]*

## 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

# Alarm and Activation

## Alarm – what types of incidents?

Further detail the types of incidents and the organisational areas that this plan relates to.

Describe how the incident can be identified. What monitoring is in place? What threats can lead to what type of incident?

Who and what triggers the activation of this plan? Not all incidents will require a response via an Incident Response Team.

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.

Describe in what situations the incident needs to be escalated. For example, can the incident escalate to a crisis and the Vice Chancellor or Chair of the Crisis Management Team must be informed to consider activating the Crisis Management Plan?

## Activation

Describe how it is decided to activate this plan and by whom.

Describe how the relevant team members are informed. E.g., do they have all the contact numbers programmed into their own mobile?

## The Incident Response Team (IRT)

The IRT is the following team but depending on the situation specific members can be added or can replace the mentioned members. The chair can already set this in motion during a first assessment and it can be decided by the team in a first gathering.

It is recommended to identify for each role within the team a secondary person who can fulfil the role in case the primary cannot attend.

|  |  |  |
| --- | --- | --- |
| **Position/stream leads** | **Primary** | **Alternate** |
| Lead/Chair |  |  |
| Note taker/log keeper |  |  |
| Consider a facilitator |  |  |
| Consider a communication coordinator |  |  |
| Subject area one |  |  |
| Subject area two |  |  |
| Subject area three |  |  |
| …. |  |  |
| …. |  |  |

[It is practical to include telephone numbers of the team members. However, there are considerations both for and against doing this. Do what suits best.]

# Command, Control and Communication

## Command

### Command hierarchy

Describe authorities and delegations of the IRT and if required, how and when it needs to obtain authorisation.

Describe if any teams are already predefined for contingency solutions and for recovery.

### Meeting point: location of the IRT

There is a high likelihood that incidents may take place outside business hours or when staff are out of the e office or travelling hence the major mechanism for coordination is via virtual meeting i.e., Zoom which is the University preferred mechanism.

If required, the physical meeting location is:

|  |  |
| --- | --- |
| **Address** | **Room** |
|  |  |

If 24x7 coordination is required, consider setting up a roster for the IRT.

## Control

### Standard agenda

Always coordinate with other teams involved in the incident or related incidents!!!

| **Topic** | **Agenda Item** | **Assigned** |
| --- | --- | --- |
| Review the facts | * What do we know about the incident? (time, date, location(s), expected or known root cause, expected duration) * Status of who/what is impacted * Response at scene / by resolver team(s) * Update from management or other related teams | Chair |
| Team membership | * Who else should be involved? * Do we have the right people? | Chair |
| Establish priorities | * What are our current exposures? * Which critical business processes and stakeholders are impacted? * What actions are being taken / should be taken? * What additional resources are required? | All |
| Next Steps | * Confirm action required * What items need to be aligned with other teams? * Agree time and date for next meeting | Chair |

### When does this team stand down?

Once the incident is under control and recovery has come to an end, the team will stand down.

However, before the IRT is stood down, the team should review the incident and record the lessons learned.

This will be used to update the IRT and contingency/recovery plans.

It can also be fed into a review of the risks analysis or can be used for other risks controls.

### Reporting, minutes, decision/action log

A note taker will be added to the team so to take the meeting minutes and keep a log of decisions made by the team. Use the following template for the decision/action log.

|  |  |  |  |
| --- | --- | --- | --- |
| Nr | Date/time | Decision or action | Action owner |
|  |  |  |  |
|  |  |  |  |

## Communication

A communication coordinator is appointed who will arrange any coordination with stakeholders.

Communicate to stakeholders regarding the incident and the selected response. If this is normally not expected of the response team, a simple question to the person who authorises the response 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.

Also communicate progress and completion.

# Critical Processes and Recovery Priorities

It is possible that the response to the incident might need to vary per incident scenario. In that case, model the response accordingly.

## Priorities

Health and safety of people takes priority. At any time WHS directions and emergency response take precedent.

Identify which contingency measures and/or recovery strategies need to be taken to minimise disruption, further risk, maximise continuity and start the recovery to normal.

## Critical processes

The list below shows the critical processes, services or activities that have priority for recovery or in case of an incident.

| **#** | **Critical process** | **Recovery Time Objective** | **Response Priorities /**  **Contingencies** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Contingency/recovery strategies and requirements

1. **IT systems Contingency/Recovery Requirements**

Outlined below is a summary of IT system used by each of the processes with strategies, contingency plans or recovery plans should these be unavailable.

| **Process** | **IT system** | **Strategies or Plans** if system or application is unavailable |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. **Location or Equipment**

Outlined below are critical business processes that rely on specific location(s), and strategies or plans should the location or specialist equipment be unavailable.

| **Process** | **Location or Equipment** | **Strategies or Plans** if location or equipment is unavailable |
| --- | --- | --- |
|  |  |  |
|  |  |  |

All other critical business processes do not require specialist equipment and in the event of a denial of access to a location, will relocate to an alternate location (either another WSU site or work remotely from home).

1. **Third Party Contingency/Recovery Requirements** (Vendors, Suppliers and Partners)

Outlined below are critical business processes that rely on material third parties and strategies should the third party be unavailable.

|  |  |  |
| --- | --- | --- |
| **Critical Business Process** | **Provider(s)** | **Strategies** if third party is unavailable |
|  |  |  |
|  |  |  |

All other critical business processes included in this plan are not reliant on material third parties.

1. **Dependent Third Parties**

Outlined below are third parties that depend on our services or facilities. Their business activities might also be impacted and therefore contingency and recovery activities need to be aligned with them. Those parties might have their own response teams.

|  |  |  |
| --- | --- | --- |
| **Third party** | **Facility or service** | **Relationship Manager** |
|  |  |  |
|  |  |  |

## Metrics

It is essential that decisions are based upon timely, accurate, and relevant data. The table below is a guide to those metrics and calendar dates that may inform the continued response, noting that as the situation develops further, metrics may become desirable to track.

| **Critical Business Process** | **Metrics** | **Key Date / Milestone** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 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.

Sometimes, the contingency solution can be described using a single sentence or a few words, e.g., “working from home”. In other cases, you might need a separate document. The same applies to recovery.

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 and focusses on bringing order into chaos. Business Continuity Plans always work under the umbrella of the Crisis Management Plan but have a narrower scope and focus more on managing the continuity and recovery.

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 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 * TRTS Business Recovery Response Plan – Hawkesbury Campus |
| Moderate or Minor Incident | * Incident Response Plan | * Teaching and Research Technical Services (TRTS) - Building Alarm Response Plan; Bldg. 24 CTN 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.