Incident Response Solutions

Incident Response Plan

Introduction

- We have provided a sample from our templated Incident Response plan (*section A*) to assist you in either starting or improving your plan.
- We have provided examples of best practice throughout the template, but you will need to consider what works best for your organisation.
- We recommend that you consult your in-house experts and seek our assistance if required.

Click here if you wish to create a tailored cyber incident response plan

Incident Response Plan Full Version – Contents

Section A – Preface (Approximately 2 pages)
– Document Control
– Testing and Updates

Section B – Cyber Incident Response Policy (Approximately 5 pages)
– Introduction
– Purpose
– Cyber Incident Response Team (CIRT) Personnel
– Incident Prioritisation
– What is a Cyber Incident?
– What is a Privacy Breach?
– External Reporting
– Ongoing Monitoring

Section C – Cyber Incident Response Procedure (Approximately 12 pages)
– Phase 1 – Preparation
– Phase 2 – Detection & Analysis
– Phase 3 – Containment, Eradication and Recovery
– Phase 4 – Post Incident Activity

Incident Response Plan Sample – Section A – Preface

- **Document Control**

This plan defines the Organisation's steps for responding to a cyber incident. The plan as published is to be communicated to all active members of the Computer Incident Response Team (CIRT). All CIRT members will retain an up to date printed copy of this document. This document has been compiled in accordance with incident response best practice.

Version	Notes	Author	Approvals
1.0	First Edition	IRS	IRS on 01/08/19
2.0	Minor Review	IRS	IRS on 22/02/20
3.0	Major Review (NZ Privacy Act 2020)	IRS	IRS on 19/01/21
4.0	Minor Review	IRS	IRS on 27/05/22
5.0	Minor Review	IRS	IRS on 12/12/22
6.0	Minor Review	IRS	IRS on 19/05/23

- **Testing and Updates**

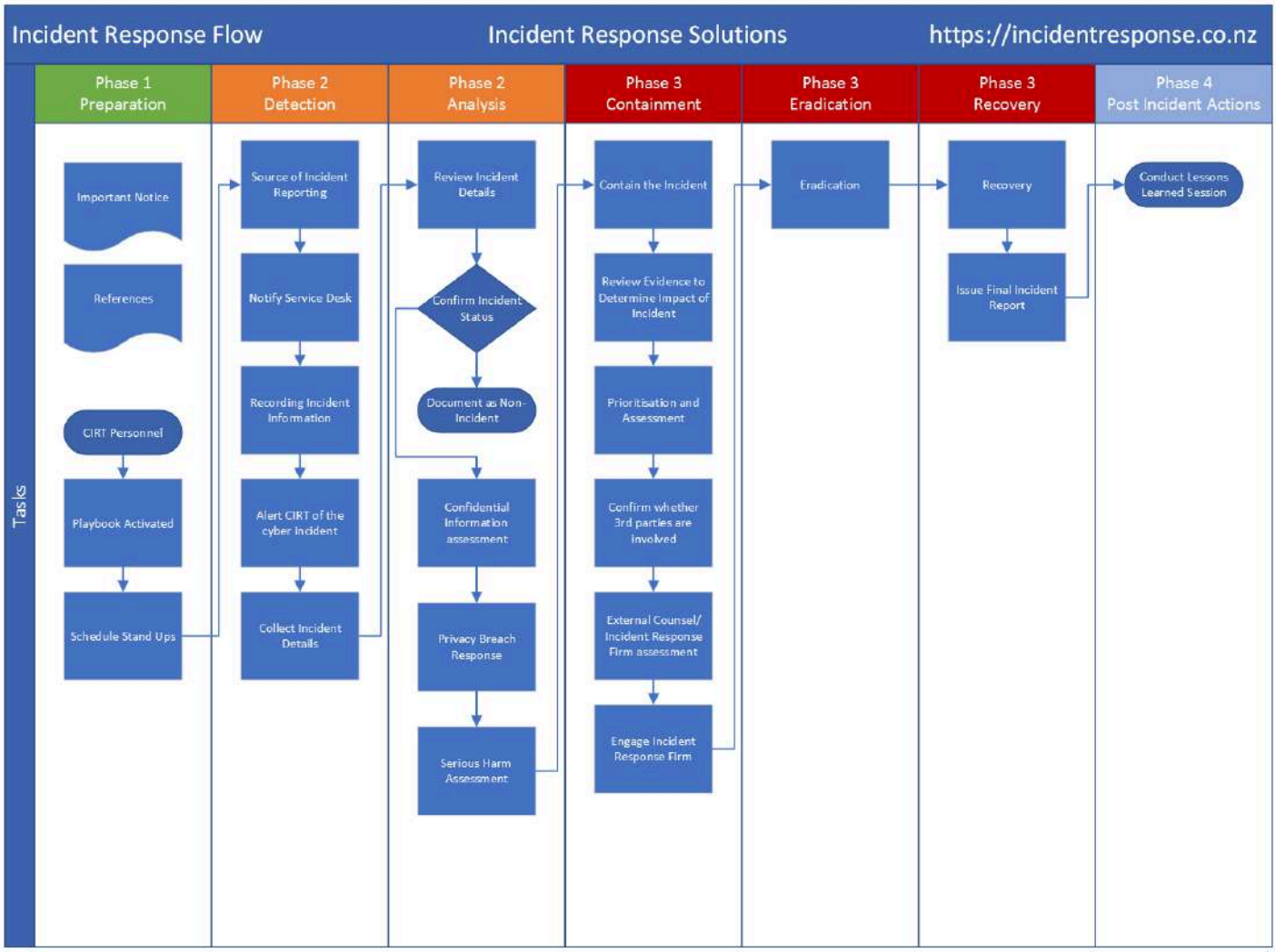
This cyber incident response plan will be tested and updated regularly to prepare for potential cyber incident scenarios and to identify areas for improvement. Review of this plan will be triggered by any of the below:

- A Post Incident Review (PIR) that identified a critical or high severity failing.
- A PIR or cyber simulation that identified a requirement to review the plan.
- A failed test or audit of the plan, policy or procedure.
- Otherwise at a minimum, at least once per year.

The Head of IT Security is responsible for:

- Planning and initiating the testing of this plan, at least annually, by way of a table-top simulation or similar. A real incident may be considered as fulfilling this requirement.
- Ensuring that the CIRT are continually aware of their obligations.
- Assigning a team member to record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.
- Conforming with industry standards and complying with regulatory requirements.
- Ensuring the incident response plan is updated and distributed to CIRT members.

The screenshot below provides an overview of the remainder of the Incident Response Plan available from Incident Response Solutions.



Click here if you wish to create a tailored cyber incident response plan

Our Incident Response Plan and full set of associated Cyber Playbooks are hosted in an electronic control room which is hosted in a cloud solution. Read more on our Control Room offering here.

We can also assist you in drafting a Business Continuity Plan (BCP) and Disaster Recovery Plan (DR).

Or contact us here.