<Organisation Name>

Cyber Security Incident Communications Plan [Template]

<Document Version & Date>



Copyright © 2021 <Organisation Name>

This document is based on a template document provided by Real World Technology Solutions.

Real World Technology Solutions grants permission for the template document to be modified in any manner <Organisation Name> wishes, provided this acknowledgement remains in place.

Document Owner: <Person’s Name>

Contact: <Person’s email and/or mobile telephone>

**How to use this template document**

This is a template document. It contains suggested or recommended content.

It is content that can be freely added to, moved, modified, or deleted.

Do not feel obliged to use the content as is if it does not suit your organisation.

You should read and adopt, adapt or remove, as appropriate!

What to do:

1. This document uses generic text for certain items that need to be updated by the organisation. These template text items are formatted in red with angle brackets (e.g. <Organisation Name> representing the organisation’s name), and should be updated to replace the template text with appropriate text specific to the organisation.
2. Using global replace, change <Organisation Name> to the organisation’s name
3. On the front page and in the page headers, change the Document Title to remove
“ [Template]” from the title, if present
4. On the front page and in the page footers, update the <Document Version & Date> to a new version of this document after your editing, and as you edit it in the future; e.g. V1.5 2025-05-05
5. Edit the document header to include the organisation’s logo, or remove the <Organisation Logo> template text
6. Find any other template text items and update them with the appropriate text for the organisation
7. Sometimes <there will be additional usage guidance formatted in blue like this comment> – it provides guidance and a reminder that the content can be freely edited to make it appropriate for your organisation
8. Review all the content and change anything as required to meet the organisation’s requirements and circumstances – sections and text can be modified, moved, deleted or added
9. Update the Contents table after updates by clicking on “Contents” and “Update Table…”; you may occasionally be prompted and can “Update entire table”
10. When ready, delete these instructions on this page and update the Contents again
11. Save the updated document

Contents

[1 This Plan 5](#_Toc88123771)

[2 Preparations Checklist 5](#_Toc88123772)

[3 Incident Handling 5](#_Toc88123773)

[3.1 Incident Response and Recovery 5](#_Toc88123774)

[3.2 Post- Incident 6](#_Toc88123775)

[3.3 Things to Communicate 6](#_Toc88123776)

[3.4 Reporting the Incident 6](#_Toc88123777)

[3.5 Media Communications 6](#_Toc88123778)

[4 Review – Accurate and Current 6](#_Toc88123779)

# This Plan

This is the Cyber Security Incident Communications Plan for <Organisation Name>. Use it to communicate effectively during any cyber security incident. Because cyber attacks can make access to electronic files impossible, **PRINT** this document, making sure the printed version is always the latest version available.

# Preparations Checklist

Use this checklist to prepare for a cyber security incident and be ready to execute this Plan.

<This is an example list of information – add, delete, modify as needed>

* <Communications App (e.g. Telegram, WhatsApp, Signal)> will be used during an incident
* <Communications App (e.g. Telegram, WhatsApp, Signal)> has been installed on the mobile telephones of <List of People>
* The <App channel or group name; e.g. OurEmergencyChannel> has been created in <Communications App (e.g. Telegram, WhatsApp, Signal)> for use in an incident
* <List of people> have provided the following personal information (see table below):
	+ Mobile telephone number
	+ Alternate (non-organisational) email address
	+ Chat application usernames (e.g. @MyNameIsMartha)
	+ Normal out-of-hours location (e.g. suburb or address)
* This Plan is printed and replaces any previously printed document.

<This table is an example of what might be useful, including example content – add, delete and modify sections as needed, and then add appropriate content>

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Person | Role | Location | Email | Chat Name | Telephone |
| Henry Reims | Vicar | North Ridge | henry@home.au | @Henry | 0499 555 111 |
| Sandra Silk | Office Mgr | South Point | sally@isp.org | @SuperSandy | 0499 111 555 |
| Peter Ponto | MSP Inc | City | peter@msp.com | @MSP\_PeterP | 0499 345 789 |

# Incident Handling

## Incident Response and Recovery

<This is an example list of information – add, delete, modify as needed>

* Immediately remove <System names> from the network, if still connected
* Telephone <Name of Person> to advise a cyber security incident is in progress
* Telephone <External Organisations> who will assist with resolving the incident
* Advise <Regulatory or Mandatory Reporting Authorities>, if required
* Provide updates to <List of People> <every two hours> until fully resolved
* Do not use email on any system or telephone until advised by <Name of Person> that it is OK to do so

## Post- Incident

<This is an example list of information – add, delete, modify as needed>

* Telephone <List of People> to advise the cyber security incident is ended
* Telephone <External Organisations> who assisted for any final advice and to thank them
* Advise <Regulatory or Mandatory Reporting Authorities>, if required
* Provide a report to <Group of People> within <four weeks> after incident is resolved, including lessons learned

## Things to Communicate

Some important things to communicate may include:

* <This is an example list of things – add, delete, modify as needed. See Examples below.>
* Date and time of first awareness of incident, and milestones to resolution
* Known effects of incident – keep these current as they change or are better understood
* Known impact on normal activities – keep this current as it changes or is better understood
* Summary of people actively involved or requested to be involved in working the incident
* Estimated date/time of activities until incident resolution, as they become clear, including:
	+ Activities to reduce the effects and impact of the incident
	+ Understanding of the cause of the incident
	+ Resolution activities in progress
	+ Essential functions/services/activities preserved or restored
	+ Incident fully resolved
	+ Non-essential functions/services/activities restored
* Any actions or decisions required of <List of People>
* <Other relevant matters>

## Reporting the Incident

<Note: As with all sections, only if required>

After the incident is fully resolved, log it on the Australian Government Cyber Reporting website:

<https://reportapp.cyber.gov.au/#/business>

## Media Communications

Only <Name of Person> will communicate with the media, if required. Refer all enquiries to <Name of Person>. Guard sensitive information extremely carefully, particularly if asked questions.

# Review – Accurate and Current

This Plan can only be effective if the details in it are kept accurate and up-to-date. This Plan is reviewed every six months to ensure the details it contains remain accurate and current, but it should be revised and updated at any time to keep it accurate and current.