<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 Introduction 6](#_Toc88123333)

[1.1 Scope 6](#_Toc88123334)

[1.2 Associated Plans 6](#_Toc88123335)

[1.3 Printed! 6](#_Toc88123336)

[2 Preparations Checklist 7](#_Toc88123337)

[2.1 Essential Preparations – Checklist 7](#_Toc88123338)

[3 Incident Workflow 8](#_Toc88123339)

[3.1 Initial Response to an Incident 8](#_Toc88123340)

[3.2 Recovery and Restoration 8](#_Toc88123341)

[3.3 Post- Incident 8](#_Toc88123342)

[4 Means of Communication 9](#_Toc88123343)

[4.1 Essential Preparations 9](#_Toc88123344)

[4.1.1 General Communications Information 9](#_Toc88123345)

[4.1.2 Communications Applications 9](#_Toc88123346)

[4.2 IT Network Communications 9](#_Toc88123347)

[4.3 Telecommunications 10](#_Toc88123348)

[4.4 Email 10](#_Toc88123349)

[5 EXECUTE THIS PLAN! [Actions] 11](#_Toc88123350)

[5.1 Use Telecommunications 11](#_Toc88123351)

[5.2 Immediate Communications 11](#_Toc88123352)

[5.3 Update Communications During Incident 13](#_Toc88123353)

[5.4 Update Communications Post-Incident 13](#_Toc88123354)

[6 EXECUTE THIS PLAN! [Checklist] 14](#_Toc88123355)

[6.1 Incident Information 14](#_Toc88123356)

[6.2 Use Telecommunications 14](#_Toc88123357)

[6.3 Immediate Communications 14](#_Toc88123358)

[6.4 Update Communications During Incident 14](#_Toc88123359)

[6.5 Update Communications Post-Incident 15](#_Toc88123360)

[7 Executive Communications 16](#_Toc88123361)

[7.1 Executive Personnel 16](#_Toc88123362)

[7.2 Staying Up-to-date 16](#_Toc88123363)

[7.2.1 Content 16](#_Toc88123364)

[7.2.2 Frequency 17](#_Toc88123365)

[8 Internal Communications 18](#_Toc88123366)

[8.1 Internal Personnel 18](#_Toc88123367)

[8.1.1 Content 18](#_Toc88123368)

[8.1.2 Frequency 18](#_Toc88123369)

[9 External Communications (Service Providers and Suppliers) 19](#_Toc88123370)

[9.1 External Contacts 19](#_Toc88123371)

[9.1.1 Content 19](#_Toc88123372)

[9.1.2 Frequency 19](#_Toc88123373)

[9.1.3 Protocol 19](#_Toc88123374)

[10 External Communications (Interested Parties) 20](#_Toc88123375)

[10.1 Interested Parties Contact Information 20](#_Toc88123376)

[10.1.1 Content 20](#_Toc88123377)

[10.1.2 Frequency 20](#_Toc88123378)

[10.1.3 Australian Federal Police 20](#_Toc88123379)

[10.2 Interested Parties Acceptable Communications Information 21](#_Toc88123380)

[10.2.1 Media 21](#_Toc88123381)

[11 Review – Accurate and Current 22](#_Toc88123382)

[12 Example Communications 23](#_Toc88123383)

[12.1 <Organisation Executive Group Name> 23](#_Toc88123384)

[12.2 Internal Personnel 24](#_Toc88123385)

[12.3 External Organisations Assisting Resolution 25](#_Toc88123386)

[12.4 External Interested Parties 26](#_Toc88123387)

# Introduction

This is the Cyber Security Incident Communications Plan for <Organisation Name>. It defines what must happen to communicate effectively during any cyber security incident. It is especially important to follow this Plan closely during a major cyber security incident, particularly if the Business Continuity Plan is invoked. (See the Business Continuity Plan for more details on that Plan.)

## Scope

This Plan is focused on cyber security. Whilst there are many other events that this Plan could be used for, including fire, flood, civil disturbance, etc, this Plan does not explicitly cover them. Nevertheless, the Plan does have aspects that are common to any adverse event, and therefore can be helpful in a broader set of communications planning activities.

This Plan covers all operations of <Organisation Name>.

## Associated Plans

This Plan is intended to be used with other Plans that define activities for various purposes, including:

* <This is an example list of documents – add, delete, modify as needed>
* Cyber Security Incident Response Plan
* Cyber Security Incident Recovery Plan
* Business Continuity Plan
* <Other relevant documents>

This Plan is executed in conjunction with related Plans as indicated throughout those documents.

## Printed!

This Plan and all associated Plans that are needed during a cyber security incident **must be printed**, ensuring the **latest version** is always the one available in printed form. This is required because cyber security incidents commonly make access to electronic files problematic or impossible.

**ALWAYS CHECK** the Document Date and Version of the PRINTED document to ensure it is the latest version!

# Preparations Checklist

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

NOTE: This checklist is **not** the Plan to be executed. Chapter 5 below (EXECUTE THIS PLAN!)
is the Plan to execute!

## Essential Preparations – Checklist

Use this checklist to prepare for any eventual cyber security incident.

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

* Communications applications to be used in various incident scenarios have been identified and obtained, as needed [See Section 4.1.2 below (Communications Applications) for a selection of possible applications]
* Personnel have installed required communications applications on mobile <and desktop> devices, as appropriate
* Relevant groups/channels have been created in the chosen communications applications
* Personnel have provided the following personal information to the organisation:
	+ Mobile telephone number
	+ Landline telephone number, if available
	+ Organisation email address
	+ Alternate (external) email address
	+ Chat application usernames (e.g. @MyNameIsMartha)
	+ Normal out-of-hours location (e.g. suburb or address) [if on-call]
* Personnel information provided above is entered into the appropriate **printed** documentation that will be available during an incident
* This Plan has been printed and replaces any previously printed document.

# Incident Workflow

## Initial Response to an Incident

This is the workflow during the initial response to a suspected or actual cyber security incident.

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

* Working with the <Organisation Cyber Security Manager>, confirm a cyber security incident is in progress and identify the type of incident
* Understand if or how the organisation’s IT network has been affected, and the effects, scope and impact of the incident
* Using the telecommunications network and approved applications, Inform the following personnel of the incident:
	+ Essential internal personnel who will be needed to respond to and manage the incident
	+ Any external organisation who will be needed to assist with responding to or managing the incident
	+ <Organisation Executive Group Name>
	+ All personnel who are or will be affected by the incident
	+ Any external organisations who are or will be affected by the incident
* Provide updates to the above people and groups at regular, prescribed intervals

## Recovery and Restoration

This is the workflow during the full response to and recovery from an incident, including restoration of all functions, services and normal operational activities.

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

* Updates provided to <Organisation Executive Group Name> at prescribed intervals
* Updates provided to these, as required:
	+ Internal personnel
	+ External personnel assisting resolution
	+ External organisations and people affected by the incident
	+ External interested parties (e.g. media)

## Post- Incident

This is the workflow after restoration of normal operations and an incident is closed.

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

* Updates provided to these, as required:
	+ Internal personnel
	+ External personnel assisting resolution
	+ External organisations and people affected by the incident
	+ External interested parties (e.g. media)
* Final written Report on Incident provided to <Organisation Executive Group Name> no later than <seven days> after incident is resolved, including lessons learned

# Means of Communication

Cyber security incidents are notorious for disrupting normal means of communication. This Plan must use appropriate, effective means of communicating even when normal means have been disrupted.

## Essential Preparations

The following preparations are required to try to ensure effective communications during a cyber security incident.

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

### General Communications Information

Internal personnel will ensure that their current details, as noted in Section 2.1 above (Essential Preparations – Checklist), are provided to the <Organisation Cyber Security Manager> (or delegate) and any changes to these are notified in a timely manner. On-call personnel should also provide the normal out-of-hours (general) location where they can be reached.

### Communications Applications

Internal personnel will install the following applications on their mobile devices and keep them up-to-date. These same applications may also be installed on desktops, if desirable.

<You may decide that NO such applications are safe to use in a cyber security incident – if that is so, simply document that here.>

* <This is an example list of applications – add, delete, modify as needed>
* Telegram – use <Telegram Channel or Group Name> (this is the primary application for communications during an incident)
* Signal – use <Signal Channel or Group Name>
* WhatsApp – use <WhatsApp Channel or Group Name>
* Slack – use <Slack Channel or Group Name>
* Zoom – use <Zoom Channel or Group Name>
* <Application Name> – use <Application Name Channel or Group Name>
* <Application Name>
* <Other relevant applications>

## IT Network Communications

Communications that use the organisation’s IT network must be viewed with extreme suspicion during any cyber security incident. Networks are the highways that propagate cyber security incidents – it is essential to exercise a high degree of caution and suspicion about the integrity of the organisation’s IT network until the scope and nature of the incident are well understood. The <Organisation Cyber Security Manager> will decide what activities, if any, can be performed on the IT network.

**Do NOT use the IT network during any suspected or actual cyber security incident unless advised to do so by the <Organisation Cyber Security Manager>!**

## Telecommunications

Cyber security incidents can disrupt telecommunications activities if they use the organisation’s IT network; e.g. Internet-based telephones. However, incidents within an organisation do not generally disrupt mobile network telecommunications provided by major commercial network providers.

It is reasonable to immediately switch to using mobile telecommunications platforms during an incident. This could be voice or SMS or mobile communications applications.

The warning below about the use of email still applies even with externally-hosted email reached via mobile networks. It is the email itself that can be a potential threat!

## Email

Email is frequently a vector of cyber security incidents and even if email is not obviously disrupted, it must still be viewed with suspicion. It is possible for an email to start an incident, and by sending additional email on the matter, one may actually propagate the incident to other people and systems!

If the scope and nature of any incident clearly do not involve or affect email, it can be used for communications. This determination must be made by the <Organisation Cyber Security Manager>.

**Use significant caution with email during any
suspected or actual cyber security incident!**

# EXECUTE THIS PLAN! [Actions]

In the many and varied possible scenarios that cyber security incidents present, it may be difficult to communicate effectively. Nevertheless, the approach below provides options to take when any cyber security incident is identified. Execute this Plan!

<This is an example list of actions, many of which may be required – add, delete, modify as needed>

## Use Telecommunications

Cyber security incidents often impact IT networks. Unless otherwise advised by the <Organisation Cyber Security Manager>, do **NOT** use the IT network – use **only** the telecommunications network when a cyber security incident is suspected or confirmed.

1. Communicate using the following as appropriate:
	1. Mobile telephone (voice or SMS)
	2. <Group chat application name> in the <Chat group or channel name> via the telecommunications network
2. Where required and approved by the <Organisation Cyber Security Manager>, communicate using email via the telecommunications network

## Immediate Communications

**Using only approved, safe communications methods**, communicate appropriately as detailed below.

1. All internal personnel
	1. Immediately inform all personnel that an incident is (or may be) in progress
	2. See table of contact information in Section 8.1 below 7.1 below(Internal Personnel)
	3. Provide relevant incident information – see Section 8.1.1 below (Content)
	4. Advise all personnel to **immediately stop using the IT network for any purpose**
	5. Advise all personnel to shutdown or remove systems from the IT network
2. Essential internal personnel needed to respond to and manage the incident
3. Immediately inform that an incident is in progress
4. See table of contact information in Section 8.1 below 7.1 below(Internal Personnel)
5. Provide relevant incident information – see Section 8.1.1 below (Content)
6. Obtain confirmation of any commitments required from personnel
7. <Organisation Executive Group Name>
8. Immediately inform that an incident is in progress
9. See table of contact information in Section 7.1 below (Executive Personnel)
10. Provide relevant incident information – see Section 7.2.1 below (Content)
11. Ensure <Organisation Executive Group Name> is fully aware of any decisions required from them and there is a clear timetable for those decisions
12. If <Organisation Executive Group Name> declares this is a major incident and invokes the Business Continuity Plan, use that Plan as the context in which to continue executing this Communications Plan.
13. Any external organisation needed to assist with responding to or managing the incident
14. As soon as possible in the circumstances, using the agreed protocols for communicating with the external organisation, contact the organisation
15. See table of contact information in Section 9.1 below 7.1 below(External Contacts)
16. Provide relevant incident information – see Section 9.1.1 below (Content)
17. Obtain confirmation of any obligations and actions required from the external organisation
18. All internal personnel who are or will be affected by the incident
19. Immediately inform that an incident is in progress
20. See table of contact information in Section 8.1 below 7.1 below(Internal Personnel)
21. Provide relevant incident information – see Section 8.1.1 below (Content)
22. Obtain confirmation of any commitments required from personnel
23. Any external organisations or individuals who are or will be affected by the incident
24. As soon as is reasonably possible, whilst managing the immediate effects of the incident, using the agreed protocols for communicating with the external organisation, inform the organisation of the incident
25. See table of contact information in Section 10.1 below 7.1 below(Interested Parties Contact Information)
26. Provide relevant incident information – see Section 10.1.1 below (Content)
27. Inform and reassure actions are being taken – do not elaborate
28. External Regulatory or Mandatory Reporting Authorities
29. As soon as is reasonably possible, whilst managing the immediate effects of the incident, using the agreed protocols for communicating with the <relevant group>, inform the <relevant group> of the incident
30. See table of contact information in Section 10.1 below 7.1 below(Interested Parties Contact Information)
31. Provide relevant incident information – see Section 10.1.1 below (Content)
32. Inform and seek any advice on relevant matters
33. Australian Federal Police <Note: As with all these sections, only if needed or required>
34. As soon as is reasonably possible, whilst managing the immediate effects of the incident, using the agreed protocols for communicating with the AFP, inform the AFP of the incident
35. See table of contact information in Section 10.1 below 7.1 below(Interested Parties Contact Information)
36. Provide relevant incident information – see Section 10.1.1 below (Content)
37. Inform and seek any advice on known responses and actions to take
38. An alternative to direct contact can be to log the incident here:

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

External interested parties do **not** need to be contacted in the initial response.

## Update Communications During Incident

Once initial immediate communications have been made, provide update communications as follows at the intervals specified or the duration from the start of the incident.

1. <Organisation Executive Group Name>
2. After 30 minutes: Advise current status and any additional decisions required
3. After one hour: Advise current status, activities in progress, and timelines
4. After three hours: Update current status, activities in progress, and timelines
5. Every 12 hours: Update current status, activities in progress, and timelines
6. Internal personnel
7. After 30 minutes: Advise current status, activities in progress, and timelines
8. As Needed: Update current status, activities in progress, and timelines
9. Every 24 hours: Update current status, activities in progress, and timelines
10. External organisations assisting with the incident
11. After 30 minutes: Advise current status, activities in progress, and timelines
12. As Needed: Update current status, activities in progress, and timelines
13. Every 24 hours: Update current status, activities in progress, and timelines
14. External people and organisations affected by the incident
15. After three hours: Advise current status and timelines
16. As Needed: Update current status and timelines
17. Every 48 hours: Update current status and timelines
18. External interested parties
19. After six hours: Advise current status
20. As Needed: Update current status and timelines

## Update Communications Post-Incident

Once the incident has been fully resolved, provide update communications as follows.

1. <Organisation Executive Group Name>
2. After one hour: Advise resolution status and any additional decisions required
3. After three days: Initial written report and summary of event
4. After seven days: Final written report
5. Internal personnel
6. After one hour: Advise resolution status and any consequential activities
7. External organisations assisting with the incident
8. After one hour: Advise resolution status and any consequential activities
9. External people and organisations affected by the incident
10. After three hours: Advise resolution status
11. External regulatory or mandatory reporting authorities and AFP
12. After three hours: Advise resolution status
13. External interested parties
14. After six hours: Advise resolution status

# EXECUTE THIS PLAN! [Checklist]

This Checklist can be printed and used to track actions during execution of this Plan in actual cyber security incidents.

<This is an example checklist based on the example list of actions, many of which may be required – add, delete, modify as needed. Keep this aligned with the detail of EXECUTE THIS PLAN! [Actions]>

## Incident Information

Incident ID:

Incident Type:

Date/Time Detected:

## Use Telecommunications

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Action | Status/Done | Time |
| 1 | Switched to telecommunications | ✓ | 07:35 |
| 2 | Email via telecommunications approved/disallowed? | Disallowed | 07:35 |

## Immediate Communications

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Action | Status/Done | Time |
| 3 | Contacted ALL internal personnel | ✓ | 07:36 |
| 4 | Contacted essential internal personnel | ✓ | 07:37 |
| 5a | Notified <Organisation Executive Group Name> | ✓ | 07:39 |
| 5b | <Organisation Executive Group Name> declared Major Incident? | Yes | 07:42 |
| 5c | <Organisation Executive Group Name> invoked BCP? | NO | 07:42 |
| 6 | Contacted <external organisation providing assistance> |  |  |
| 7 | Advised affected internal personnel |  |  |
| 8 | Contacted <external organisation affected> |  |  |
| 9 | Contacted <Regulatory authority> |  |  |
| 10 | Contacted AFP |  |  |

## Update Communications During Incident

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Action | Status/Done | Time |
| 11 | Updated (@30 mins): <Organisation Executive Group Name> |  |  |
| 12 | Updated (@30 mins): Internal personnel |  |  |
| 13 | Updated (@30 mins): <External organisation assisting> |  |  |
| 14 | Updated (@3 hrs): <External organisation/people affected> |  |  |
| 15 | Updated (@6 hrs): <External interested party (e.g. media)> |  |  |
| … | <Additional updates> |  |  |
| … | <Additional updates> |  |  |
| … | <Additional updates> |  |  |

## Update Communications Post-Incident

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Action | Status/Done | Time |
| 16 | Updated <Organisation Executive Group Name> |  |  |
| 17 | Updated Internal personnel |  |  |
| 18 | Updated <External organisation assisting> |  |  |
| 19 | Updated <External organisation/people affected> |  |  |
| 20 | Updated <External regulatory or mandatory reporting authorities> and <AFP> |  |  |
| 21 | Updated <External interested party (e.g. media)> |  |  |
| … | <Additional updates> |  |  |
| … | <Additional updates> |  |  |
| … | <Additional updates> |  |  |

# Executive Communications

This Cyber Security Incident Communications Plan for <Organisation Name> defines what must happen to communicate effectively during any cyber security incident. It is crucial to keep <Organisation Executive Group Name> informed of the progress of the incident.

## Executive Personnel

This Plan requires good and regular communications with <Organisation Executive Group Name> whose details follow:

<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 |
| Cecelia Reims | CEO | North Ridge | ceci@our.org | @Ceci | 0499 555 111 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Staying Up-to-date

The executive personnel listed above will receive regular communications during any major cyber security incident. Because <Organisation Executive Group Name> is responsible for declaring that a major cyber security incident is in progress, and therefore invoking the Business Continuity Plan, it is crucial that <Organisation Executive Group Name> is kept up-to-date with the status of any cyber security incident that is or potentially may be classified as “major”. It is the responsibility of the <Organisation Cyber Security Manager> to ensure <Organisation Executive Group Name> is kept informed of such incidents.

To avoid confusion and ensure continuity of communication with <Organisation Executive Group Name>, all communications with <Organisation Executive Group Name> will be via the <Organisation Cyber Security Manager> or delegate.

### Content

Things to put in communications with <Organisation Executive Group Name> include:

* <This is an example list of things – add, delete, modify as needed. See Examples below.>
* Incident ID
* Date and time of first awareness of incident
* Known scope of effect of incident – keep this current as the scope changes or is more fully understood
* Known impact on normal operations – keep this current as the impact changes or is more fully understood
* Summary of personnel actively involved or requested to be involved in working the incident
* Estimated date and time waypoints to incident closure as they become clear, including:
	+ Containment of the incident scope
	+ Reduction of the incident impact
	+ Understanding of the root cause
	+ Resolution activities in progress
	+ Essential functions/services/activities preserved or restored
	+ Incident resolution
	+ Non-essential functions/services/activities restored
	+ Incident closed
* Any actions or decisions required of <Organisation Executive Group Name>
* <Other relevant matters>

### Frequency

These communications will occur as frequently as needed, but not less than once every three hours during the initial incident response, and at least every 12 hours thereafter. The first notice of the incident must be made as soon as possible after it is detected, whilst rapidly engaging relevant internal and external personnel to respond to and manage the incident.

# Internal Communications

Good communications with internal personnel during a cyber security incident will help to ensure the incident is resolved as quickly and effectively as possible.

## Internal Personnel

The following table contains details of the various internal personnel who must be contacted as a cyber security incident is detected, develops, and managed to final resolution:

<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 |
| Bob Bestman | Sys Admin | Brentwood | Bestman@our.org | @Bobulous | 0499 999 888 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Individual roles may have team members that also need to be involved. The leaders of these teams may act under the authority of the <Organisation Cyber Security Manager> to communicate with and involve these team members and will keep the <Organisation Cyber Security Manager> informed of significant activities as the incident progresses.

### Content

Things to put in the communications with the internal personnel include:

* <This is an example list of things – add, delete, modify as needed. See Examples below.>
* Incident ID
* Date and time of activity
* Known scope of activity – keep this current as the scope changes or is more fully understood
* Known effect of activity – keep this current as the effect changes or is more fully understood
* Summary of personnel actively involved or requested to be involved in working the incident
* Effects and impact on personnel, if appropriate
* Estimated date and time waypoints to incident closure as they become clear, including:
	+ Resolution activities in progress
	+ Anticipated activities and timeframe of those activities
	+ Additional resources required
* Any actions required of <Organisation Cyber Security Manager>
* <Other relevant matters>

### Frequency

These communications will occur as frequently as needed, but not less than once every three hours during the initial incident response, and at least every 12 hours thereafter.

# External Communications (Service Providers and Suppliers)

Good communications with external service providers and suppliers during a cyber security incident will help to ensure the incident is resolved as quickly and effectively as possible.

## External Contacts

The following table contains details of the various external service providers and suppliers who may need to be contacted as a cyber security incident is detected, develops, and managed to final resolution:

<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>

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Organisation | Person | Role | Location | Email | Chat Name | Telephone |
| IT Help Inc | Lance Boyd | Acct Mgr | City | lb@ITHI.com | @LanceBoy | 0488 777 222 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Individual internal roles may communicate with relevant external service providers and suppliers as needed, acting under the authority of the <Organisation Cyber Security Manager> and will keep the <Organisation Cyber Security Manager> informed of significant activities as the incident progresses.

### Content

Things to put in the update communications with external service providers and suppliers include:

* <This is an example list of things – add, delete, modify as needed. See Examples below.>
* Incident ID
* Date and time of activity
* Organisation contacted and overall details of communication
* Response of the organisation
* Potential or actual activities of the organisation in the incident
* Further planned contact with the organisation
* <Other relevant matters>

### Frequency

These update communications will occur as frequently as needed, but not less than once every three hours during the initial incident response, and at least every 12 hours thereafter.

### Protocol

Communications with the external service providers and suppliers will adhere to any agreements and arrangements in place with the individual external service providers and suppliers.

# External Communications (Interested Parties)

Good communications with external interested parties during a cyber security incident will help to ensure the effects of the incident are understood by those who may be directly or indirectly affected. It will also manage the way in which the incident is understood and perceived in the wider community and media.

## Interested Parties Contact Information

The following table contains details of the various external interested parties who may be contacted as a cyber security incident is recognised, develops, and is managed and resolved:

<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>

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Organisation | Person | Role | Location | Email | Telephone |
| Media Inc | Sonya Savvy | Journalist | South Point | SonyaT@mi.com.au | 0499 123 321 |
| AFP | Frank Jones | Cyber Crime | Canberra | FJones@afp.gov | 0499 000 000 |
|  |  |  |  |  |  |

Individual internal roles may communicate with relevant external interested parties as needed, but **only** if explicitly authorised by the <Organisation Cyber Security Manager>, and will keep the <Organisation Cyber Security Manager> informed of significant communications as the incident progresses.

### Content

Things to put in the update communications with external interested parties include:

* <This is an example list of things – add, delete, modify as needed. See Examples below.>
* Date and time of activity
* Name of interested party contacted and overall details of communication
* Response of the interested party
* Any consequential activities required as a result of the response of the interested party
* Further planned contact with the interested party
* <Other relevant matters>

### Frequency

Update communications will occur as required after the initial communications. Results of sensitive communications (e.g. with media, or customers) must be made known to <Organisation Cyber Security Manager> without delay.

### Australian Federal Police

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

The <Organisation Cyber Security Manager>, in consultation with the <Organisation Executive Group Name>, will contact the Australian Federal Police as soon as the nature of the incident has been determined. An alternative to direct contact can be to log the incident here:

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

## Interested Parties Acceptable Communications Information

When communicating with external interested parties, only convey sufficient relevant information that aligns with the nature of the party’s involvement with or relationship to <Organisation Name>. Do not add information that is not relevant to the party or to which they are not entitled. Guard sensitive information extremely carefully, particularly if asked questions.

### Media

The content of communications with media organisations must be approved by <Organisation Executive Group Name>. When in contact with media organisations, do not convey information that is in any way sensitive, political or not approved for release to the media.

# Review – Accurate and Current

This Cyber Security Incident Communications Plan can only be effective if the details in it are kept accurate and up-to-date. This Plan will be reviewed at least every six months to ensure the details it contains remain accurate and current. Nevertheless, the Plan can be revised and updated at any time to keep it accurate and current.

Personnel must understand that keeping their communications details accurate and current is essential for the success of this Plan.

# Example Communications

These are some examples of possible communications to various parties.

## <Organisation Executive Group Name>

Start of incident:

<Organisation Executive Group Name> CYBER SECURITY INCIDENT FIRST NOTICE

Please be advised that a cyber security incident has been detected.

Incident ID: CSI-2025-07-24-15-55-A

Date/Time Detected: Thursday 24 July 2025 at 15.55 (Sydney)

Incident Type: SUSPECTED Ransomware attack

Status: Initial detection and analysis. Cyber Security Incident Response Plan activated.

Scope: Main database server

Current Impact: Server is offline and not available for other functions

Potential Impact: May disrupt **all services** for the **next few days**

Actions in Progress: Sys Admins analysing logs and shutting down external access to network

Next Report Scheduled: Thursday 24 July 2025 at 16.30 (Sydney)

Incident Update After One Hour:

<Organisation Executive Group Name> UPDATE NOTICE

This cyber security incident is still being responded to.

Incident ID: CSI-2025-07-24-15-55-A

Date/Time Detected: Thursday 24 July 2025 at 15.55 (Sydney)

Date/Time This Update: Thursday 24 July 2025 at 16.57 (Sydney)

Incident Type: CONFIRMED Ransomware attack

Status: Cyber Security Incident Response Plan in progress.

Scope: Main database server, customer portal, main website

Current Impact: Main database server, customer portal, and main website all offline

Potential Impact: May disrupt **all services** for the **next few days**

Actions in Progress: Sys Admins determining extent of lock out and required technical response, and clarifying hacker demands.

Next Report Scheduled: Thursday 24 July 2025 at 19.00 (Sydney)

## Internal Personnel

Start of incident:

INTERNAL PERSONNEL CYBER SECURITY INCIDENT FIRST NOTICE

Please be advised that a cyber security incident has been detected.

\*\*\* IMMEDIATE \*\*\* Action Required

Shut down ALL personal workstations NOW!!!

Incident ID: CSI-2025-07-24-15-55-A

Date/Time Detected: Thursday 24 July 2025 at 15.55 (Sydney)

Incident Type: SUSPECTED Ransomware attack

Status: Initial detection and analysis. Cyber Security Incident Response Plan activated.

Scope: Main database server

Current Impact: Server is offline and not available for other functions

Potential Impact: May disrupt **all services** for the **next few days**

Actions in Progress: Sys Admins analysing logs and shutting down external access to network

Next Update Scheduled: Thursday 24 July 2025 at 17.00 (Sydney)

Incident Update After Incident Resolution:

INTERNAL PERSONNEL CYBER SECURITY INCIDENT UPDATE NOTICE

This cyber security incident is resolved.

Incident ID: CSI-2025-07-24-15-55-A

Date/Time Detected: Thursday 24 July 2025 at 15.55 (Sydney)

Date/Time Resolved: Saturday 26 July 2025 at 02.17 (Sydney)

Date/Time This Update: Saturday 26 July 2025 at 04.30 (Sydney)

Incident Type: CONFIRMED Ransomware attack

Status: Cyber Security Incident Recovery Plan completed. Incident RESOLVED.

Scope: Main database server, customer portal, main website

Current Impact: None. Main database server, customer portal, and main website all restored to normal operations

Impact: The Ransomware attack affected **all public and customer-facing services** for 34 hours.

Resolution: Sys Admins were able to remove all ransomware and restore data from backups. Only 25 minutes of transactions from 15.30 on Thursday 24 July 2025 were lost. These can be recovered by contacting customers.

Next Update Scheduled: None.

## External Organisations Assisting Resolution

Start of incident:

<EXTERNAL Organisation Name> CYBER SECURITY INCIDENT FIRST NOTICE

Please be advised that a cyber security incident has been detected at <Organisation Name>

Incident ID: CSI-2025-07-24-15-55-A

Date/Time Detected: Thursday 24 July 2025 at 15.55 (Sydney)

Incident Type: SUSPECTED Ransomware attack

Status: Initial detection and analysis. Cyber Security Incident Response Plan activated.

Scope: Main database server

Current Impact: Server is offline and not available for other functions

Potential Impact: May disrupt **all services** for the **next few days**

Actions in Progress: Sys Admins analysing logs and shutting down external access to network

<Organisation Name> Contact: Jonah Bartholomew, 0499 777 555

Assistance Required: Contact Jonah Bartholomew IMMEDIATELY!

Incident Update During Recovery Plan:

<EXTERNAL Organisation Name> CYBER SECURITY INCIDENT UPDATE NOTICE

This cyber security incident is being worked with assistance from <EXTERNAL Organisation Name>.

Incident ID: CSI-2025-07-24-15-55-A

Date/Time Detected: Thursday 24 July 2025 at 15.55 (Sydney)

Date/Time This Update: Friday 25 July 2025 at 05.45 (Sydney)

Incident Type: CONFIRMED Ransomware attack

Status: Cyber Security Incident Recovery Plan in progress.

Scope: Main database server, customer portal, main website

Current Impact: **All public and customer-facing services** currently unavailable.

Current activities: Ransomware removed and backups to restore data scheduled to commence at 07.00 on Friday 24 July 2025 (Sydney). <EXTERNAL Organisation Name>’s <Person’s Name> onsite and assisting.

Next Update Scheduled: Friday 25 July 2025 at 09.00 (Sydney).

## External Interested Parties

Two Hours After Start of Incident:

PRESS RELEASE

At 3.55pm today, Thursday 24 July 2025, <Organisation Name> was the victim of a Ransomware attack. The attack has affected our public and customer-facing websites. At this time, we are working to establish the full extent of the attack and have engaged our external IT partners to assist with recovery of our services.

We will provide updates when we have progress to report.

Update After Incident Resolution:

PRESS RELEASE

The Ransomware attack that affected <Organisation Name> on the afternoon of Thursday 24 July 2025 has been successfully resolved. Working with our external IT partners we recovered and restored our services today, Saturday, 26 July 2025, just after 2am. We were able to disable the ransomware, remove it, and restore backups of all affected data, except for the few minutes at the start of the attack. These few minutes of data will be easily recovered with the assistance of the three customers affected.

Unlike in many Ransomware attacks, the technical staff were able to disable the attack, and <Organisation Name> did not pay any ransom. Australian Federal Police (AFP) were informed early on in the attack and have been actively involved in identifying the culprits. <Organisation Name> thanks our external IT partners, the AFP, and all who assisted in handling this event so effectively.